

Budoucnost AI a bezpečnosti ve veřejné správě

Příklad využití AI v GFŘ a jejich zabezpečení

IBM Watsonx & Fusion HCI

Michal Görtner
IBM
Customer Success Manager
michal_gurtner@cz.ibm.com

Pavol Škápik
Generální Finanční Ředitelství,
Poradce, kancelář generální ředitelky



watsonx



Doing the right AI

+

Doing AI right

IBM pomáhá organizacím komplexně a zodpovědně.



Agenda

01

Využití AI nejen v oblasti kybernetické bezpečnosti

02

Bezpečností aspekty a požadavky na AI řešení

03

GFŘ projekt Dialog (on-premise genAI)

04

Ukázka IBM řešení



Příklady AI projektů ve veřejné správě

Veřejná správa a služby pro občany

- Chatboti a **virtuální asistenti** pro komunikaci s občany (dotazy, formuláře, žádosti).
- Automatizace zpracování žádostí, registrací a licencí.
- Překladové a **hlasové služby** pro vícejazyčnou komunikaci.

Vzdělávání

- Personalizované vzdělávací materiály a učební pomůcky.
- Generování učebních plánů a adaptivní testování.
- Virtuální asistenti pro studenty a pedagogy.

Zdravotnictví

- Podpora diagnostiky a analýzy medicínských dat (AI pro snímky, laboratorní výsledky).
- Generativní AI pro sumarizaci zdravotní dokumentace.
- Virtuální asistenti pro pacienty i lékaře (navigace ve zdravotním systému, prevence, připomínky).

Doprava a infrastruktura

- Prediktivní údržba infrastruktury (mosty, silnice, železnice).
- Inteligentní řízení dopravy a optimalizace městské mobility.
- Analýza dat pro plánování veřejné dopravy.



Bezpečnost a obrana

- Prediktivní analýza kriminality, monitoring veřejného pořádku...
- Detekce kybernetických hrozeb a podvodů.
- Analýza obrazových a video dat (např. sledování hranic).

• Automatizace rutinních činností.

Otevřená data a transparentnost

- Analýza velkých objemů otevřených dat a jejich vizualizace.
- **Generování srozumitelných shrnutí** např. legislativních dokumentů.
- Podpora rozhodování na základě dat.

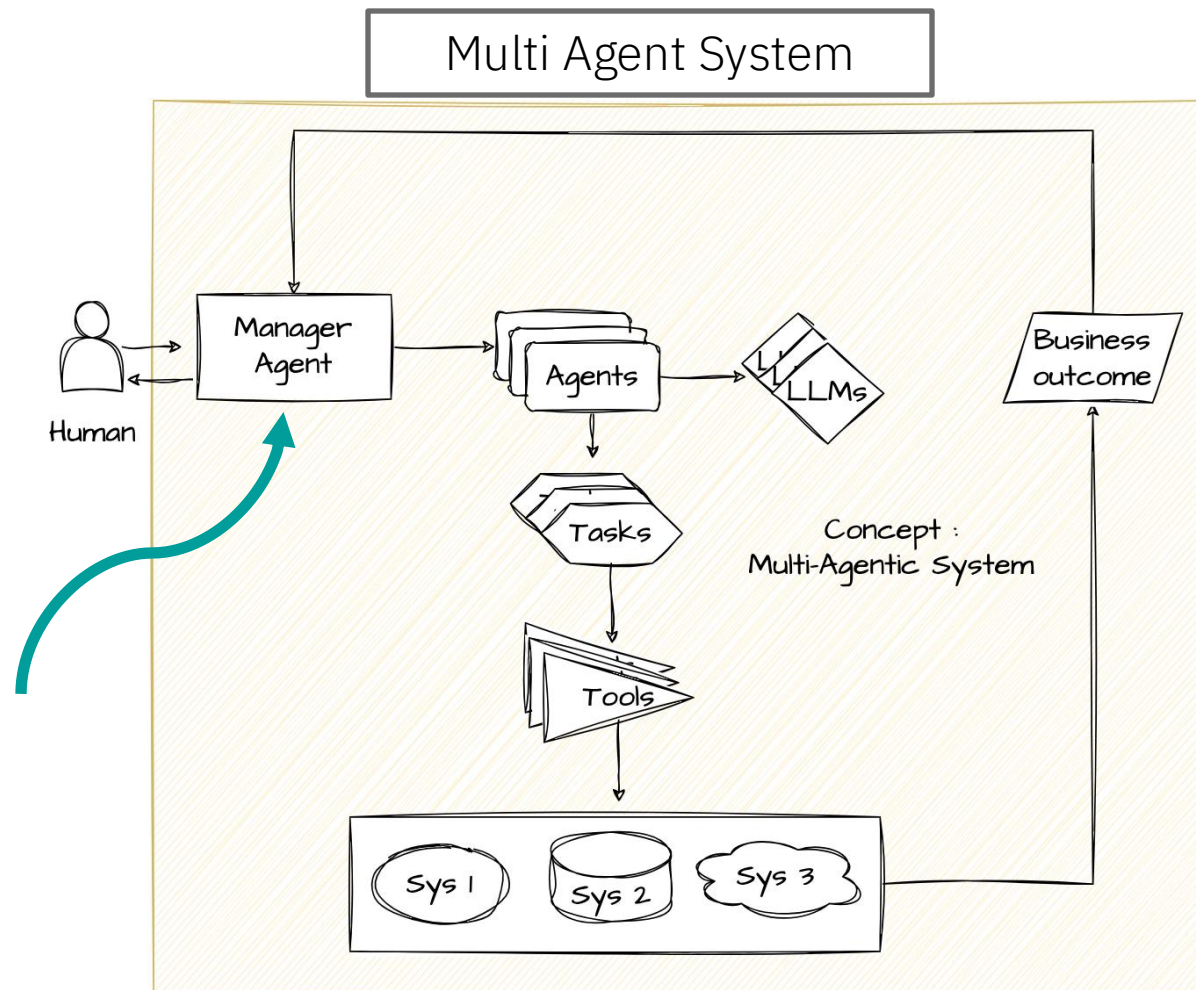
System s jedním agentem

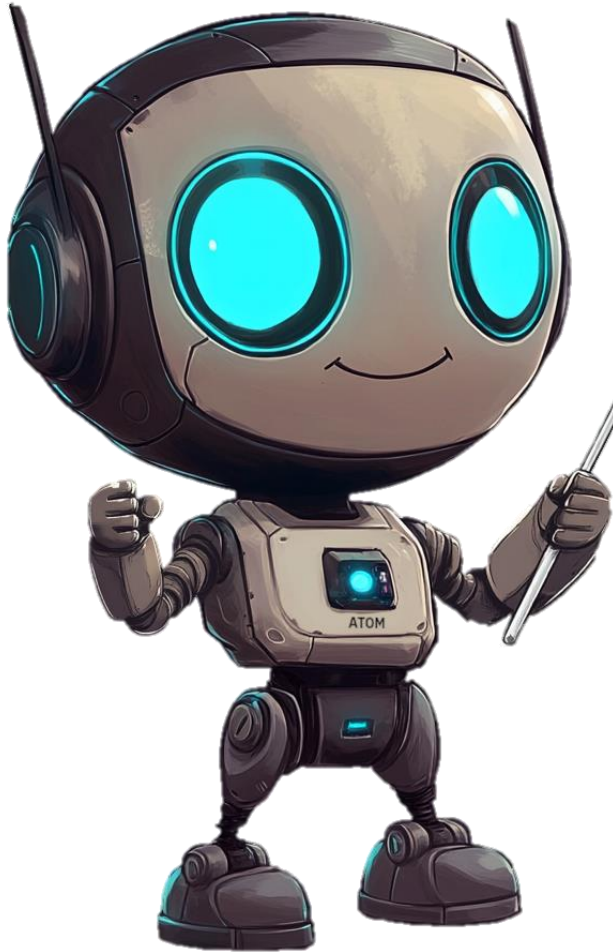
je AI systém, kde pouze jeden autonomní agent pracuje samostatně na splnění úkolu.

Multiagentní systém

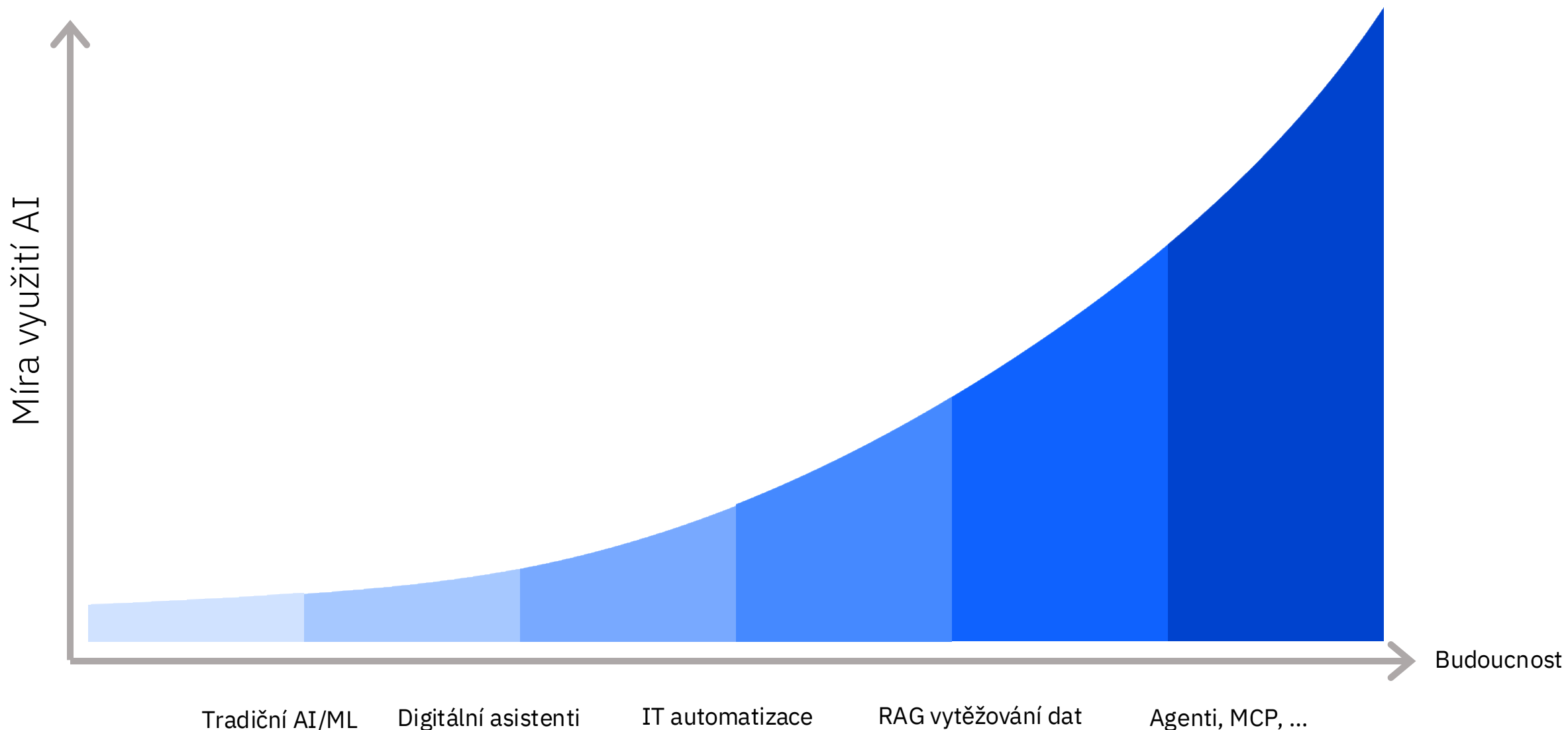
se skládá z více inteligentních agentů, kteří spolupracují na dosažení společného cíle.

ATOM je náš **AI digitální pracovník**, který řídí multiagentní systém pro řízení kybernetických hrozeb.

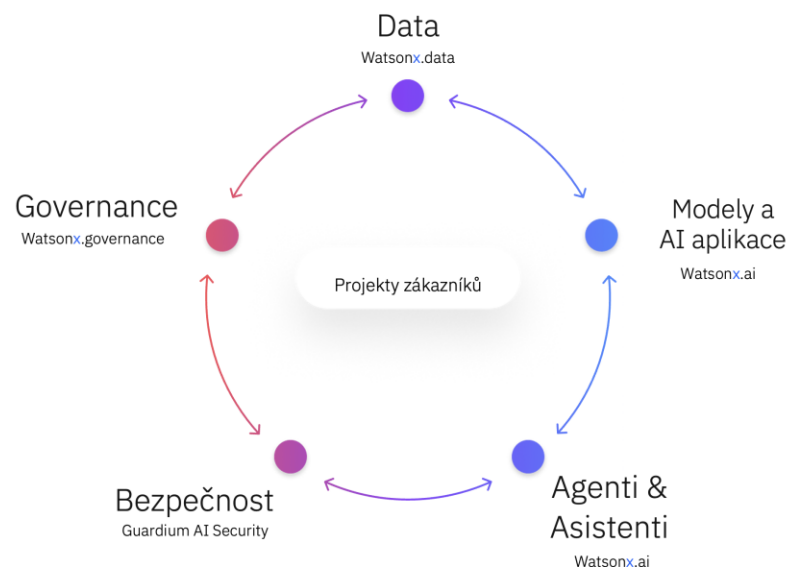




Vyšší míra využívání AI = vyšší rizika a nutnost zabezpečení



Vybrané technologie a služby



1

Infrastruktura IBM Fusion HCI

- Optimalizované prostředí HW/SW appliance IBM Fusion
- Nižší nároky na lidské zdroje a znalosti
- Možnost rozšíření na non-IBM HW

2

Platforma IBM Watsonx.AI a Cloud Pak for Data

- Podpora různých modelů
- Jednotné prostředí pro vývoj, provoz a monitoring AI řešení
- Průvodci a akcelerátory např. RAG, Chatbot, Agent builder aj.
- Modulární datový ekosystém

3

Zabezpečení IBM Guardium Security

- Ochrana dat i modelů před neoprávněným přístupem a úniky dat
- Detekce hrozeb a anomálií v chování AI systémů
- Soulad s nařízenými a efektivní AI governance



FINANČNÍ SPRÁVA

Projekt DIALOG

e-government 2025

Cloud vs. on-premise řešení

- **Cloudové AI:**

- Flexibilita, rychlé nasazení, škálovatelnost
- Nižší počáteční náklady
- Vhodné pro projekty bez přísných bezpečnostních požadavků

- **On-premise AI**

- Provoz v zabezpečené infrastruktuře (např. SP CSS)
- Vyšší nároky na HW/SW a správu
- Nevyhnutné při práci s citlivými nebo klasifikovanými daty

- **FS využívá oba přístupy podle typu projektu** – on-premise např. projekt DIALOG

Kontext projektu DIALOG

- **Digitální Analýza výsLechu a Organizace Generování**
 - protokoly o výslechu svědka / účastníka řízení představují zásadní důkazní prostředek
 - jedná se o nejnáročnější úkon při správě daní
 - emoce / zkušenost pracovníků / rizikovo verbálních útoků / riziko korupčního jednání
 - 2023: 5 452 výpovědí, 9 804 ústních jednání
 - 2024: 5 185 výpovědí, 9 745 ústních jednání
 - protokolace jednání – analýza obsahu – sumarizace do zprávy o kontrole – odvolací orgán

Současný stav

- Výslechy jsou dnes zapisované ručně, vysoká zátěž (3 300 pracovníků)
- Regionální rozdíly, zdlouhavé zpracování (měsíce)
- Relevance jen části nahrávky
- Potřeba vyhledávání, sumarizace a asistenta pro práci s věcným obsahem

Cíle projektu DIALOG

- Ověřit využitelnost AI pro
 - automatický přepis výsledků
 - test přesnosti přepisů, identifikace řečníků
 - sumarizace obsahu výsledku
 - analytika (dotazy v přirozeném jazyce)
 - identifikaci osob a udržení kontextu rozhovoru
- Ověřit technologickou, finanční a personální náročnost
 - Provoz v prostředí SPCSS (on-premise) – bezpečnost dat
 - Vytvořit základ pro nasazení dalších AI projektů ve FS
- Hlavní cíl č.1: Rychlejší a přesnější spracování dat
- Hlavní cíl č.2: Úspora nákladů a lidských zdrojů



Projekt DIALOG – Ukázka přepisu výslechu

IBM GŘ přepis jednání

Nahrávka

ZOOM H4n - překrývání.wav

IBM

0:53 8:46

Skrýt anotace

☒ Automatický posuv

Jana Kadlčíková

Dnešní jednání povedu já, Jana Kadlčíková, odborná garantka z oddělení kontrolního dva

Jana Kadlčíková

odboru kontrolního územního pracoviště v Přerově.

Ing. Šárka Kovaříková

Jako úřední osoba budu řádný průběh jednání zajišťovat rovněž já,

Ing. Šárka Kovaříková

Ing. Šárka Kovaříková, vedoucí oddělení kontrolního 2

Ing. Šárka Kovaříková

odboru kontrolního územního pracoviště v Přerově.

Michaela Balvinová

Já Michaela Balvinová zde budu dnes střežit a hájit zájmy mého klienta Stormero s.r.o.

Michaela Balvinová

z Olomouce jakožto advokát zapsaný v seznamu vedeného Českou advokátní komorou.

Mojmír Hradil

Já, Mojmír Hradil, zde budu dnes vystupovat jako svědek, jednatel společnosti Fraud Facility s.r.o., předvolaný ve věci daňového řízení společnosti Stormero

Ing. Šárka Kovaříková

Tedy vy říkáte, že jste se svým odběratelem ze Stormero uzavřel smlouvu na dálku,

Mojmír Hradil

Ano.

Ing. Šárka Kovaříková

kterou připravoval pan Houška ze společnosti Stormero a vy jste ji jen podepsal.

Mojmír Hradil

Ano, ano.

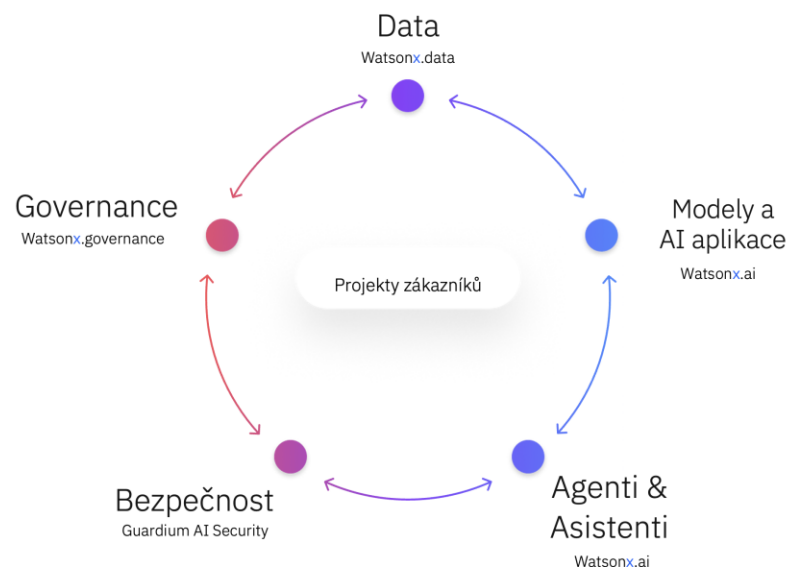
Mojmír Hradil

Je to tak.

Závěr

- Projekt DIALOG
 - **Test AI v zabezpečeném prostředí**
 - Spolupráce: **Finanční správa + IBM + SPCSS**
 - AI modely v on-premise prostředí
 - Frontend aplikace pro uživatele FS s ohledem na AD
 - Ověřujeme **technologii, finance, personální kapacity**
- Pracujeme na
 - Rozšíření AI do dalších oblastí FS
 - Nasazení jako standardní nástroj
 - Vytvoření know-how pro další AI projekty (cloud i on-premise)

Vybrané technologie a služby



1

Infrastruktura IBM Fusion HCI

- Optimalizované prostředí HW/SW appliance IBM Fusion
- Nižší nároky na lidské zdroje a znalosti
- Možnost rozšíření na non-IBM HW

2

Platforma IBM Watsonx.AI a Cloud Pak for Data

- Podpora různých modelů
- Jednotné prostředí pro vývoj, provoz a monitoring AI řešení
- Průvodci a akcelerátory např. RAG, Chatbot, Agent builder aj.
- Modulární datový ekosystém

3

Zabezpečení IBM Guardium Security

- Ochrana dat i modelů před neoprávněným přístupem a úniky dat
- Detekce hrozeb a anomálií v chování AI systémů
- Soulad s nařízenými a efektivní AI governance

IBM Fusion appliance & **watsonx**

Nejvhodnější cesta k genAI infrastruktuře v on-premises prostředí

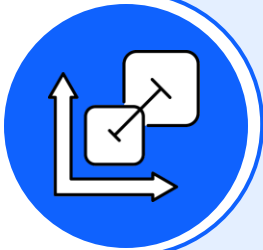


Regional mirroring, HA-zones and snapshots



Rychlé nasazení a snadná správa

- Zprovoznění systému v řádu dní vč. sw pro genAI
- Automatizovaný monitoring, zálohování a správa
- Optimalizováno pro OpenShift a genAI aplikace na Watsonx



Produkční system pro škálování genAI on-premise

- Flexibilita přidávání GPU nodů např. pro watsonx.ai inferencing, prompt tuning, training
- Připravené scénáře pro nasazení lakehouse a storage (Ceph ready)
- Flexibilita v konfiguracích a růstu CPUs, storage, cluster aj.



Vysoký výkon, datová propustnost aj.

- Benchmark Lakehouses IBM Watsonx.data – [better than Databricks at 60% cost](#)
- Nasazení watsonx na Fusion zrychlylo úlohy 7x až 90x (testy v IBM CIO office př. interní RAG aj.)

Consistent backup,
restore to another cluster



AI assistants



Data & AI
platform



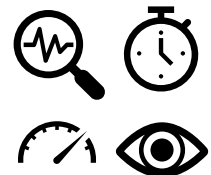
Data services



 OpenShift

IBM Fusion HCI

Monitoring,
Audit, Call home



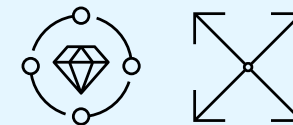
IBM Watsonx.ai

Nabízí klíčové
vlastnosti pro
budování
pokročilé AI
platformy.

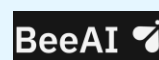
AI applications, agents and assistants



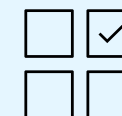
Integrated Observability and Evaluation:
AgentOps and AI/MLOps



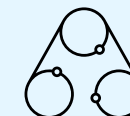
Developer toolkit:
Tools, frameworks, templates, deployments



Models



Model
Customization



Hybrid cloud platform



Red Hat



aws



AMD



Zajištění transparentnosti, bezpečnosti a důvěry v AI

Klíčové vlastnosti

Centrální repositář všech AI artefaktů Vaší organizace.

Nalézt a popsat známé i dosud neznáme AI artefakty, agenty, ...

Dodržujte požadavky na soulad s nařízeními a směrnici.

IBM software

Automatizovaný monitoring AI agentů, modelů a jiných artefaktů napříč platformami a prostředími.

Využití dalších schopností, např. klasifikace a hledání citlivých údajů.

Zabezpečení nejen AI, ale i zdrojových dat a výstupů.

The screenshot displays the IBM Guardium AI Security interface. On the left is a dark sidebar with navigation options: AI 360, AI Inventory (selected), Dashboard, Technologies, Configuration, Issues, Report, AI Usage, AI SPM, AI Gateway, AI Compliance, AI Observability, and AI Incidents. The main content area is divided into several panels. The top-left panel, 'AI PaaS Inventory' (17 Technologies), lists cloud services with columns for Technology, Resources, Org. Usage, and Review Status. The bottom-left panel, 'AI Software Inventory' (28 Technologies), lists software libraries with the same columns. On the right, there are two smaller panels: 'AI Model Inventory' (4 Technologies) and 'AI Service Inventory' (1 Technology), both showing a list of technologies.

Technology	Resources	Org. Usage	Review Status
Amazon Bedrock Machine Learning & AI	181	2	Unreviewed
Amazon SageMaker Machine Learning & AI	24	1	Unreviewed
IBM Watsonx Data Machine Learning & AI	20	2	Unreviewed
Azure OpenAI	18	1	Unreviewed
Amazon EC2 Compute Platforms	16	3	Unreviewed

Technology	Resources	Org. Usage	Review Status
FastAPI Library	3	2	Unreviewed
LangChain Library	2	2	Unreviewed
MLflow Library	2	2	Unreviewed
scikit-learn Library	2	2	Unreviewed
NumPy Library	2	2	Unreviewed

Technology
Trained ML Model A Machine Learning & AI
Google ML Model Machine Learning & AI
OpenAI Endpoint Machine Learning & AI
IBM Watsonx Endp Machine Learning & AI

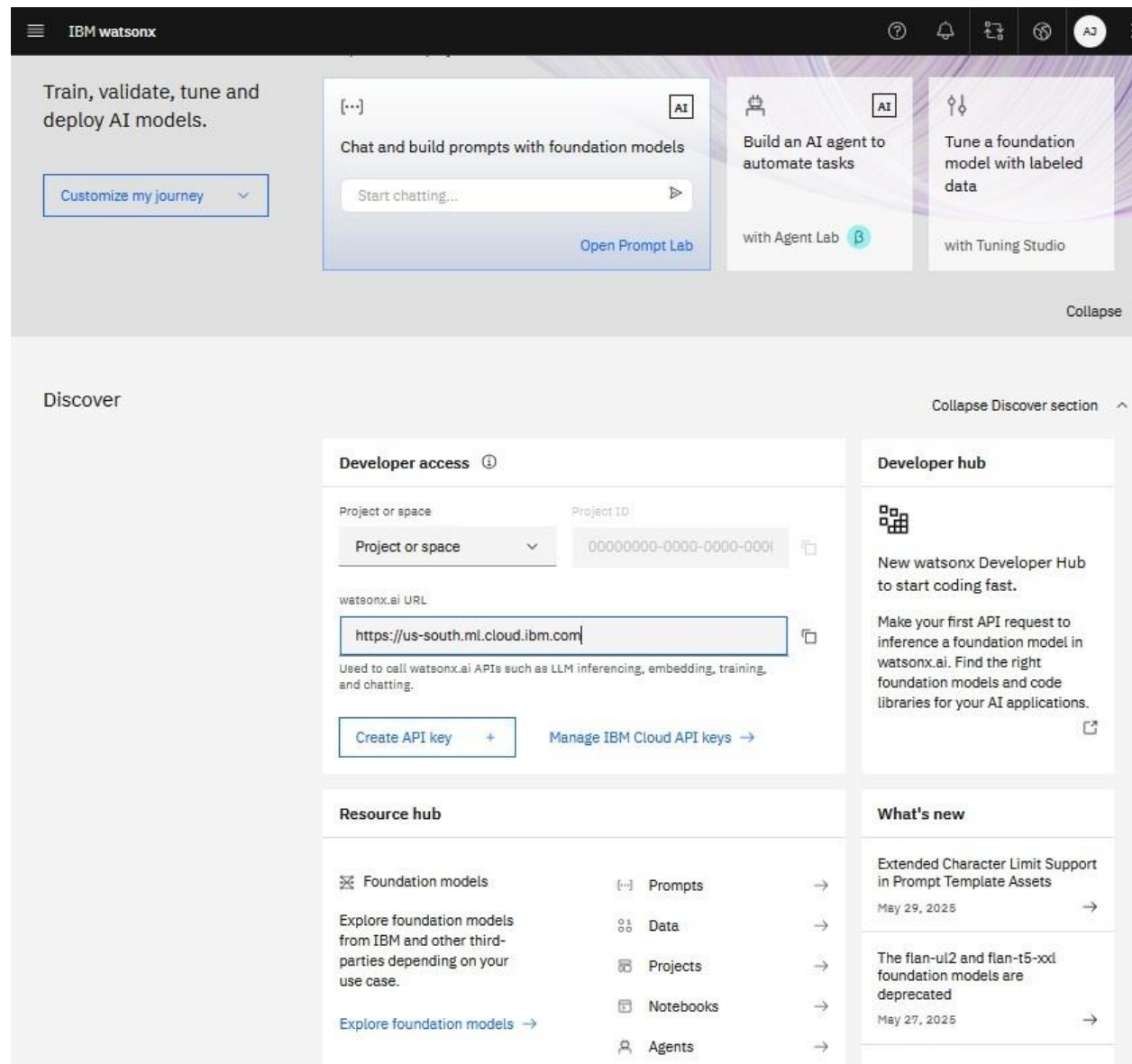
Technology
Microsoft Copilot Enterprise GenAI

IBM Watsonx Guardium Security

...

Ukázky

watsonx



Budoucnost AI a bezpečnosti ve veřejné správě

Příklady využití AI v GFŘ a jejich zabezpečení

IBM Watsonx & Fusion HCI

Michal Görtner
IBM
Customer Success Manager
michal_gurtner@cz.ibm.com

Pavol Škápik
Generální Finanční Ředitelství
Poradce, kancelář generální ředitelky

