

# Building Digital Resilience in the **AI** era

**Antonio Forzieri**

EMEA Cyber Security Specialization and Advisory







HeyGen



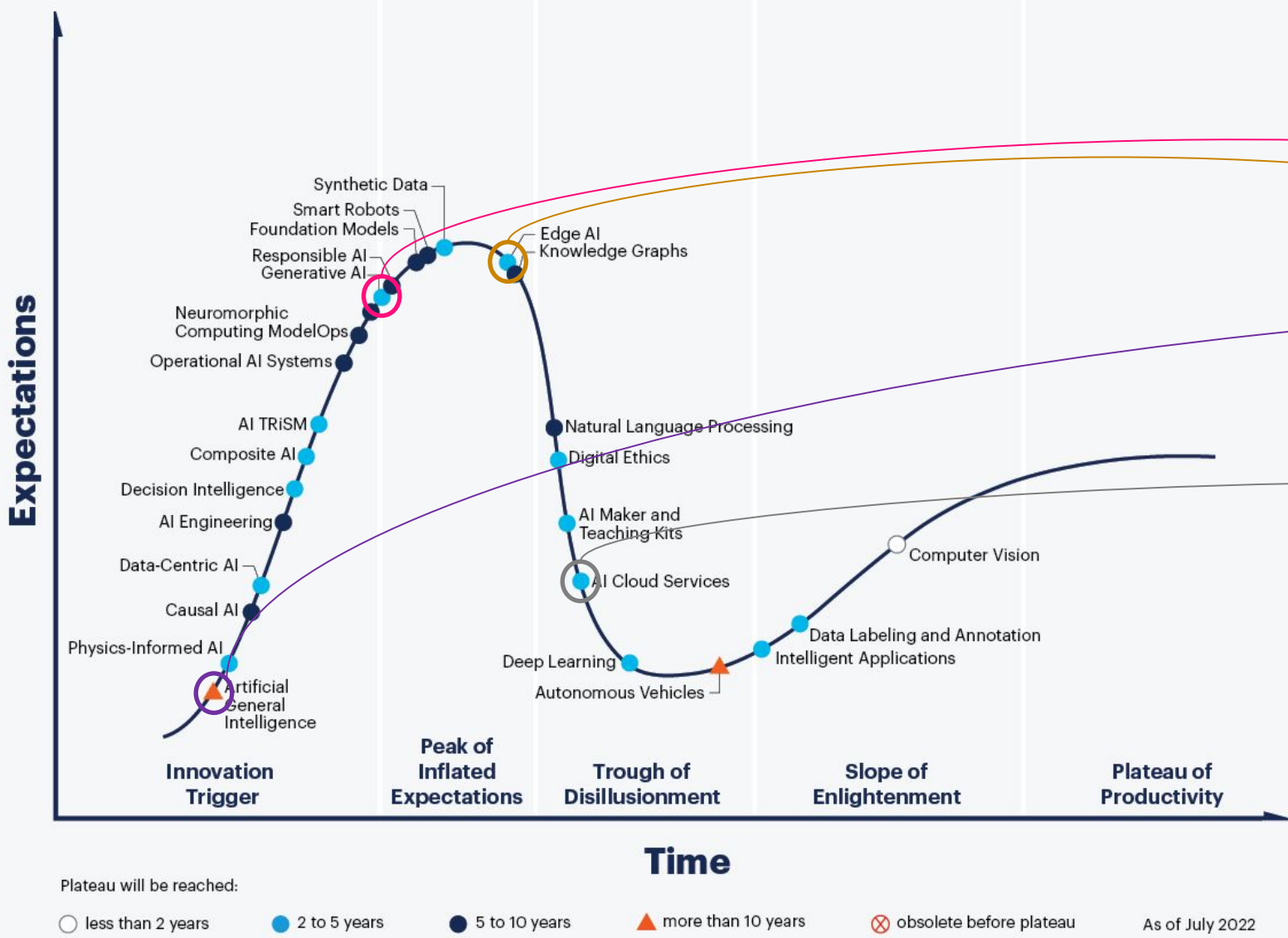


# \$ whoami

- EMEA Cyber Security Specialization and Advisory @Splunk/Cisco
- Cyber Security Director @ f3rm1 foundation
- Lecturer at Politecnico di Milano @ Network Security Class
- Build-Transform-Operate SOC ninja
- Wine lover and educated taster ONAV/AIS
- Love breaking stuff and coding
- Crazy for Special and General relativity
- Pizza maker and baker (thanks lockdown)
- EMT since 30 years
- Biker, scuba diver, crazy for power/street/whatever lifting
- X: @ilf0rz

# Where did we come from?

## Hype Cycle for Artificial Intelligence, 2022

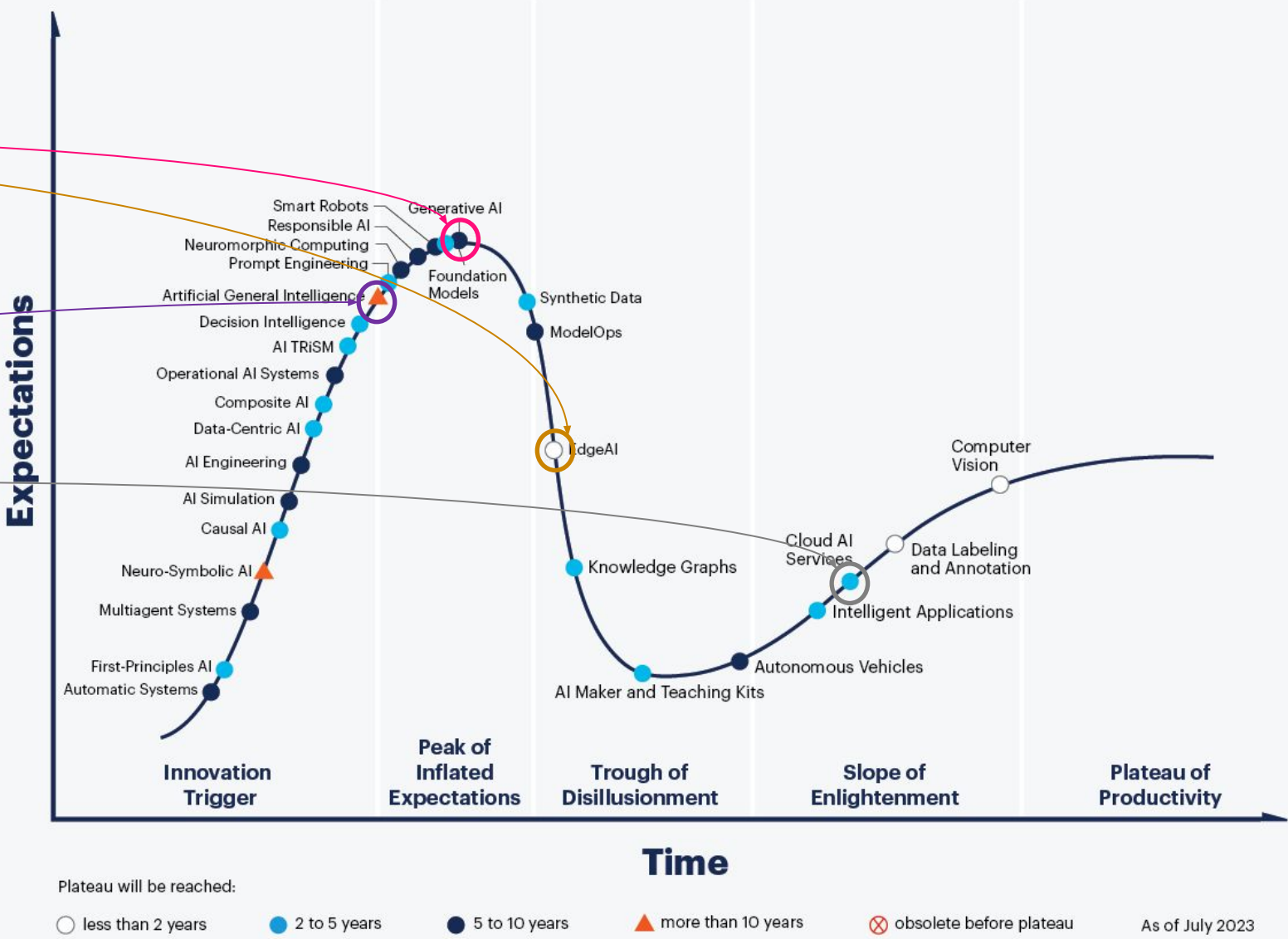


gartner.com

Source: Gartner  
© 2022 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner and Hype Cycle are registered trademarks of Gartner, Inc. and its affiliates in the U.S. 1957302

Gartner®

## Hype Cycle for Artificial Intelligence, 2023



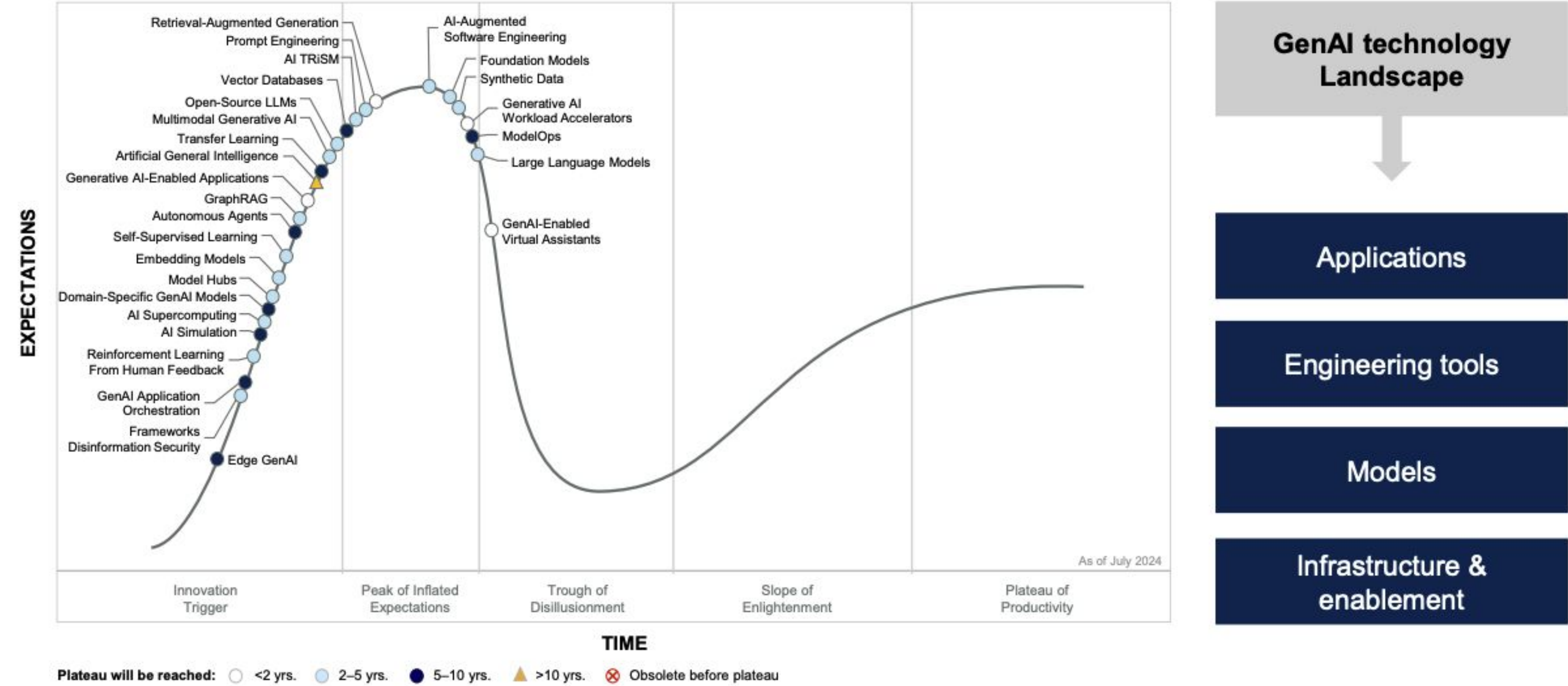
gartner.com

Source: Gartner  
© 2023 Gartner, Inc. and/or its affiliates. All rights reserved. 2079794

Gartner®



# Hype Cycle for AI in 2024





We tend to **overestimate** the effect of a technology in the short run and **underestimate** the effect in the long run.

Amara's Law

# Hype Cycle for AI in 2024

Benefit	Years to mainstream adoption			
	Less than two years	Two to five years	Five to 10 years	More than 10 years
Transformational		<ul style="list-style-type: none"><li>• AI-augmented software engineering</li><li>• AI supercomputing</li><li>• Foundation models</li><li>• Large language models</li><li>• <b>Multimodal generative AI</b></li><li>• Self-supervised learning</li></ul>	<ul style="list-style-type: none"><li>• <b>Autonomous agents</b></li></ul>	<ul style="list-style-type: none"><li>• Artificial general intelligence</li></ul>
High	<ul style="list-style-type: none"><li>• GenAI-enabled virtual assistants</li><li>• <b>Generative AI-enabled applications</b></li><li>• Generative AI workload accelerators</li><li>• <b>Retrieval-augmented generation</b></li></ul>	<ul style="list-style-type: none"><li>• AI TRiSM</li><li>• Disinformation security</li><li>• Embedding models</li><li>• Model hubs</li><li>• <b>Open-source LLMs</b></li><li>• Prompt engineering</li><li>• Reinforcement learning from human feedback</li><li>• Synthetic data</li></ul>	<ul style="list-style-type: none"><li>• AI simulation</li><li>• <b>Domain-specific GenAI models</b></li><li>• Edge GenAI</li><li>• GenAI application orchestration frameworks</li><li>• ModelOps</li><li>• Transfer learning</li><li>• Vector databases</li></ul>	
Moderate		<ul style="list-style-type: none"><li>• GraphRAG</li></ul>		

Source: Hype Cycle for Generative AI, 2024, 31 July 2024



# Deepseek and Alibaba join the party!

Rank★ (UB)	Rank (StyleCtrl)	Model	Arena Score	95% CI	Votes	Organization	License
1	2	<a href="#">Grok-3-Preview-02-24</a>	1412	+8/-10	3364	xAI	Proprietary
1	1	<a href="#">GPT-4.5-Preview</a>	1411	+11/-11	3242	OpenAI	Proprietary
3	5	<a href="#">Gemini-2.0-Flash-Thinking-Exp-01-21</a>	1384	+6/-5	17487	Google	Proprietary
3	3	<a href="#">Gemini-2.0-Pro-Exp-02-05</a>	1380	+5/-6	15466	Google	Proprietary
3	2	<a href="#">ChatGPT-4o-latest (2025-01-29)</a>	1377	+5/-4	17221	OpenAI	Proprietary
6	3	<a href="#">DeepSeek-R1</a>	1363	+8/-6	8580	DeepSeek	MIT
6	10	<a href="#">Gemini-2.0-Flash-001</a>	1357	+6/-5	13257	Google	Proprietary
7	3	<a href="#">o1-2024-12-17</a>	1352	+4/-6	19785	OpenAI	Proprietary
9	10	<a href="#">Qwen2.5-Max</a>	1336	+7/-5	11930	Alibaba	Proprietary
9	7	<a href="#">o1-preview</a>	1335	+4/-3	33167	OpenAI	Proprietary
9	10	<a href="#">o3-mini-high</a>	1329	+8/-6	9102	OpenAI	Proprietary
11	13	<a href="#">DeepSeek-V3</a>	1318	+5/-4	22007	DeepSeek	DeepSeek
12	16	<a href="#">GLM-4-Plus-0111</a>	1311	+8/-8	6035	Zhipu	Proprietary
12	15	<a href="#">Qwen-Plus-0125</a>	1310	+7/-5	6054	Alibaba	Proprietary
12	5	<a href="#">Claude 3.7 Sonnet</a>	1309	+9/-11	4254	Anthropic	Proprietary

Spource: <https://lmarena.ai/>

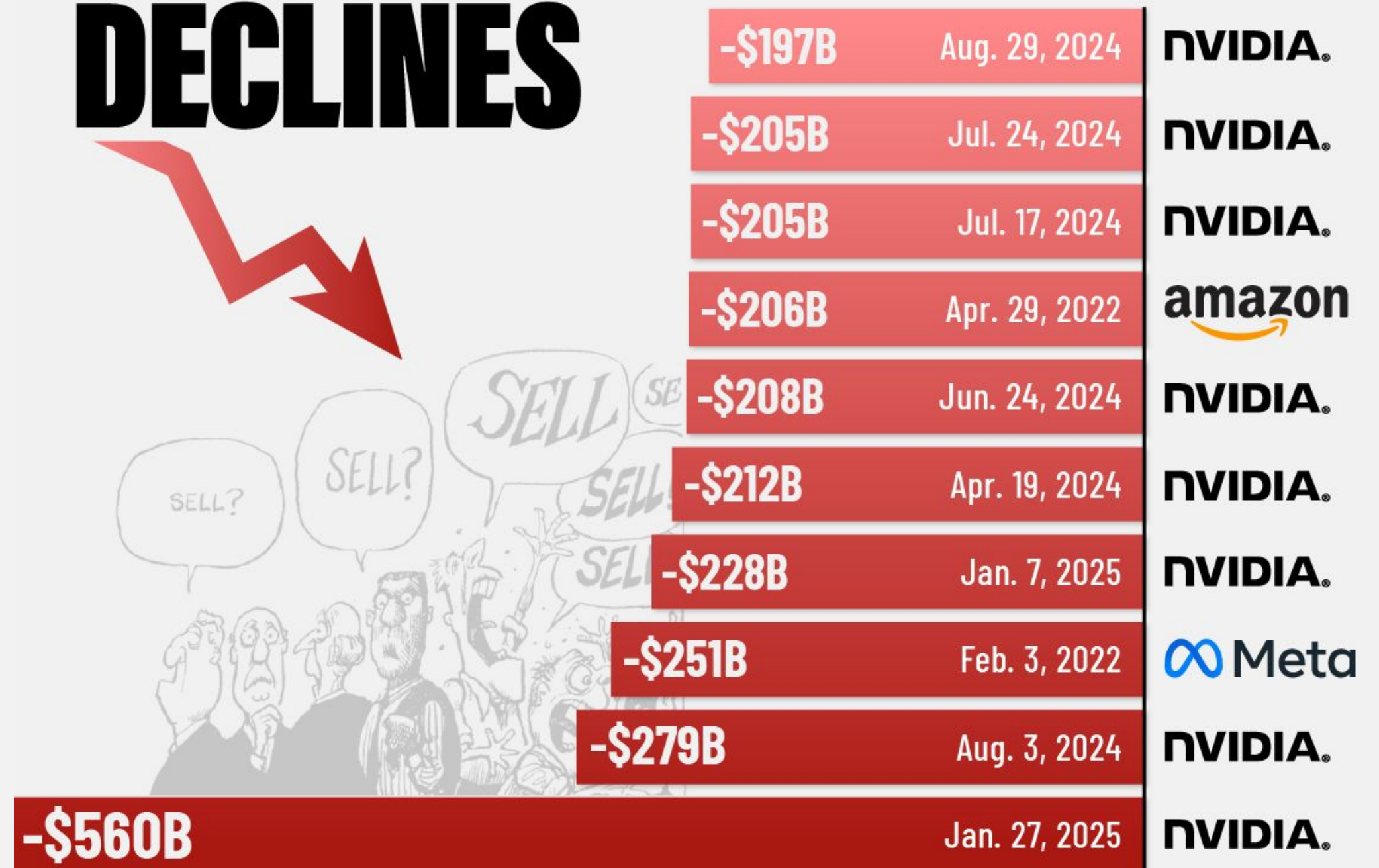




# The week that shook Silicon Valley

## THE BIGGEST SINGLE-DAY STOCK DECLINES

Nvidia has experienced 8 of the 10 biggest single-day stock declines.



Nvidia's stock plummeted after a Chinese startup called DeepSeek released a powerful AI model.

As of January 27, 2025  
Source: Bloomberg





# New Toys new Tools - Failing Fast



**Humane AI Pin**

<https://humane.com/>



**Rabbit R1**

<https://www.rabbit.tech/>



**Apple Vision Pro**

<https://www.apple.com/>

**splunk>**

**AI and Hardware**



TECH · A.I.

# HP is acquiring parts of AI Pin startup Humane for \$116 million—but retiring the product once hyped as a smartphone alternative

BY BEATRICE NOLAN

February 19, 2025 at 4:43 PM GMT+1



PHOTOGRAPHER: ANGEL GARCIA/BLOOMBERG VIA GETTY IMAGE

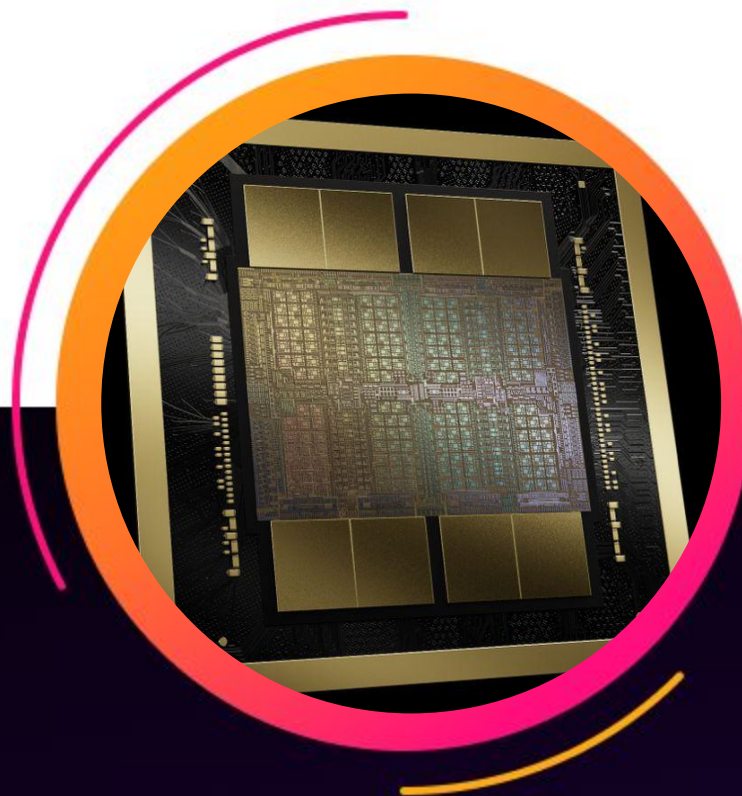


# New Toys new Tools - xPU



**Groq LPU**

<https://groq.com/>



**NVIDIA Blackwell**

<https://www.nvidia.com/>



**Apple M3/M4**

<https://www.apple.com/>

**splunk>**

**AI and Hardware**



# What am I using today?

Just to make my life easier...



**ChatGPT**



**Notebook LM**



**Copilot**



**MidJourney**



**Gemini**



**HeyGen**



**Claude AI**



**Vast AI**

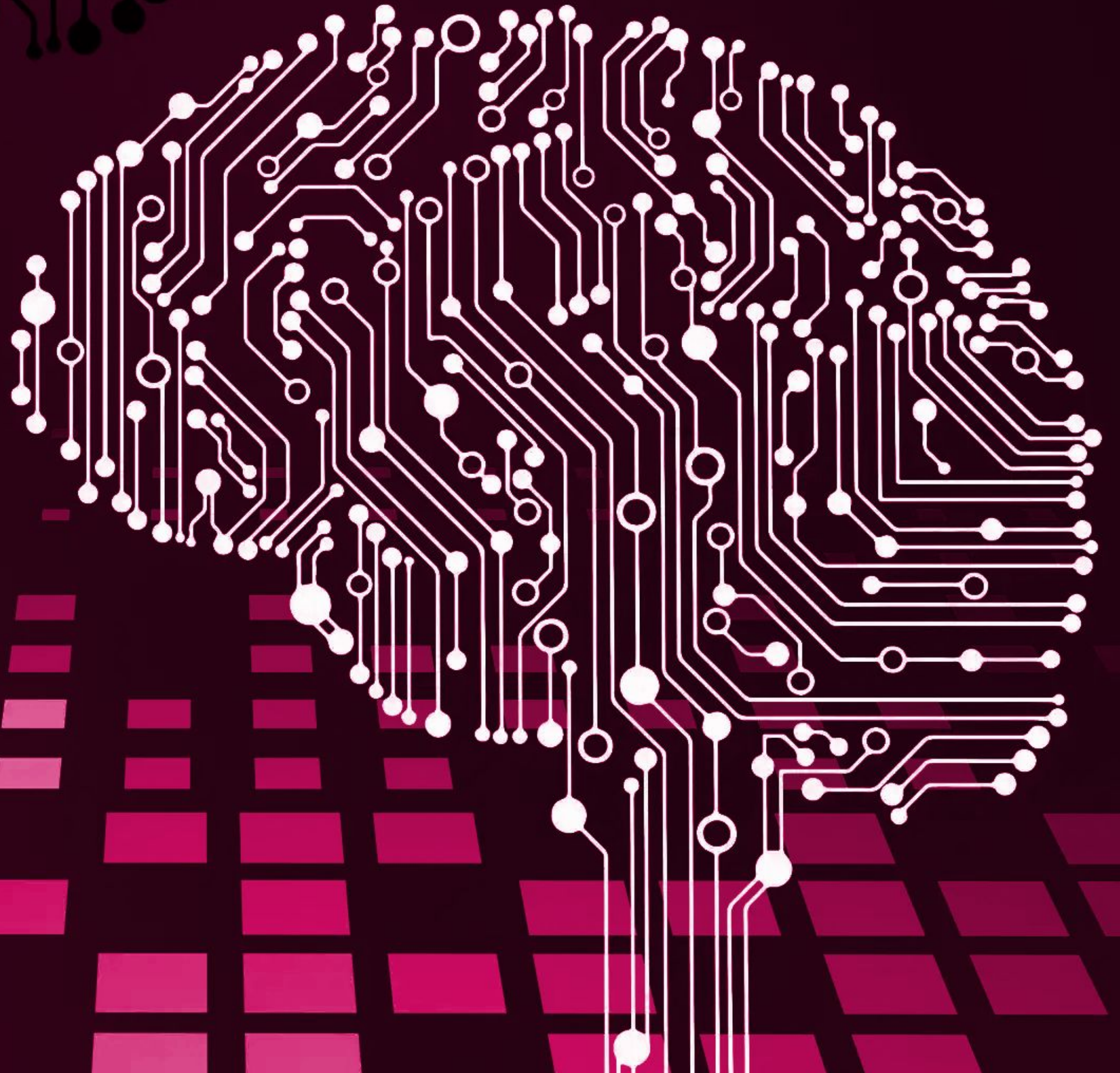


**Ollama**

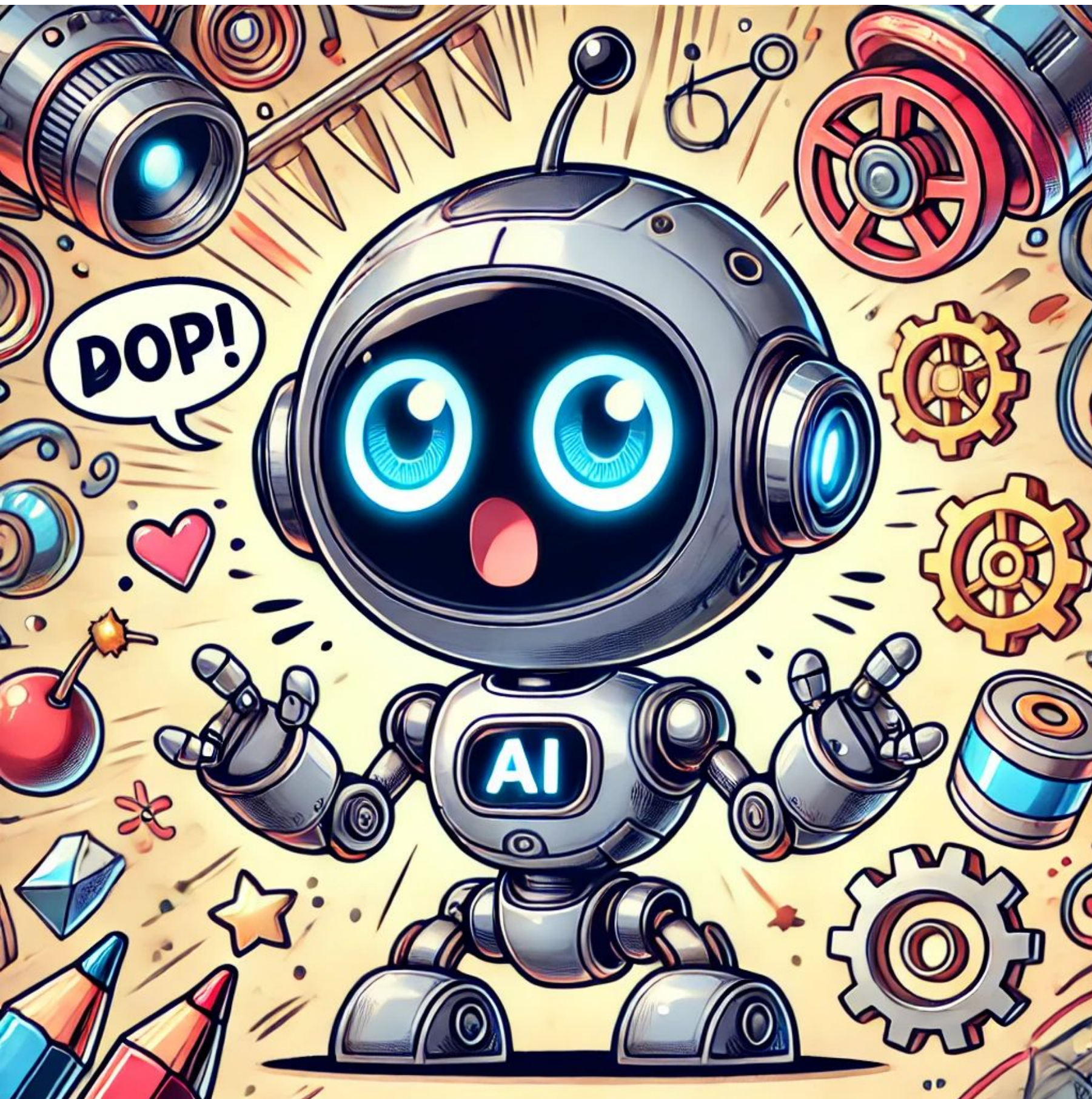




**The Next  
10 Years  
Will Be  
Shaped  
By AI  
Adoption**





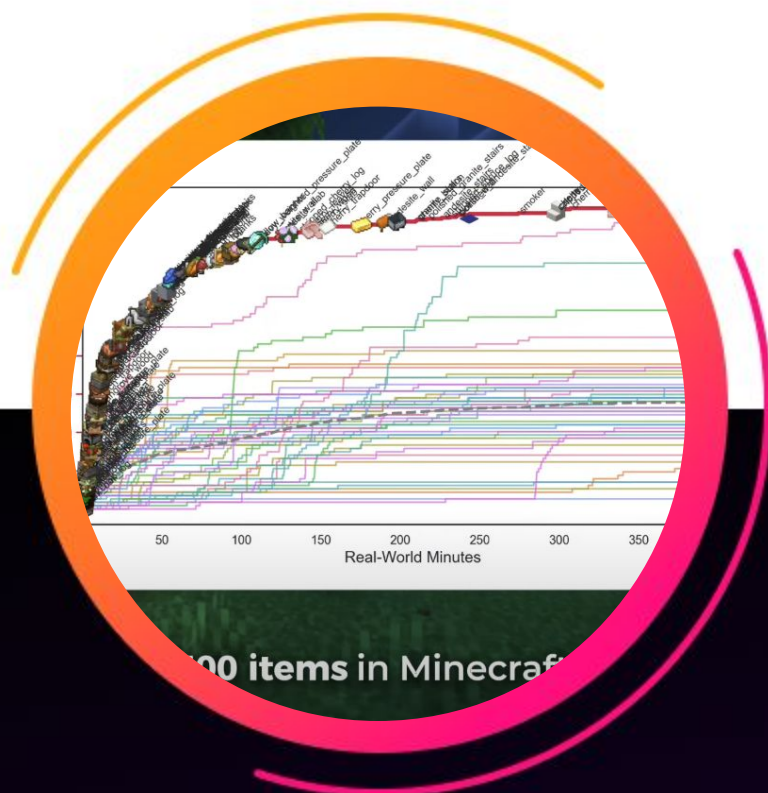


# AI Agents

- a software program that can interact with its environment, collect data, and use the data to perform self-determined tasks to meet predetermined goals.
- Humans set goals, but an AI agent independently chooses the best actions it needs to perform to achieve those goals.
- **Altera** has built **1000** AI Agents and asked them to play Minecraft. Bots:
  - Bots communicates over discord, google docs, discord, google sheet and slack



# AI Agents working together



**Agents  
collected over  
300 items.**



**Agents created  
an economy  
making  
transactions.**



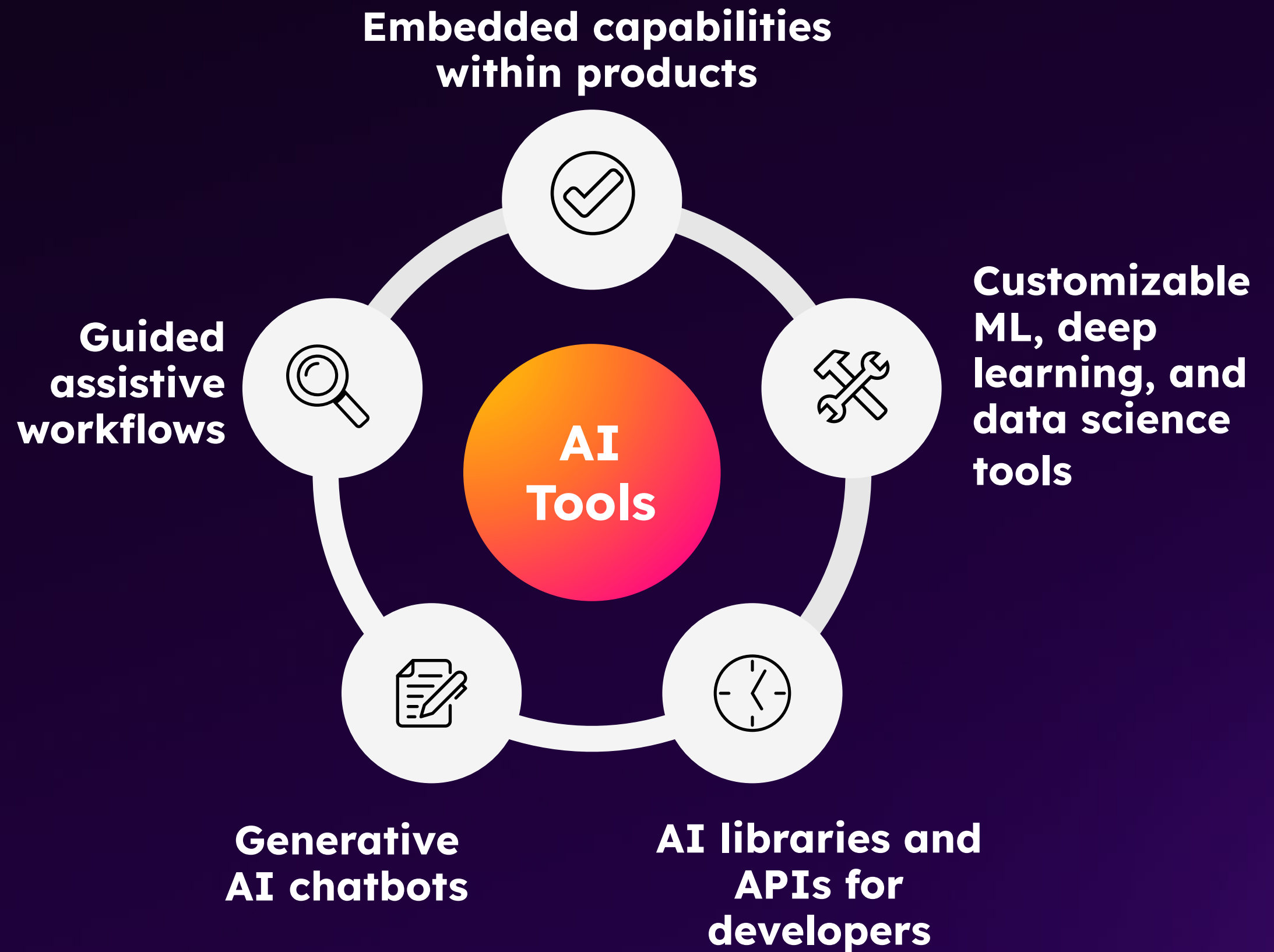
**Olivia gave up  
her dreams for  
the society.**

**splunk>**

# What about Splunk and AI?



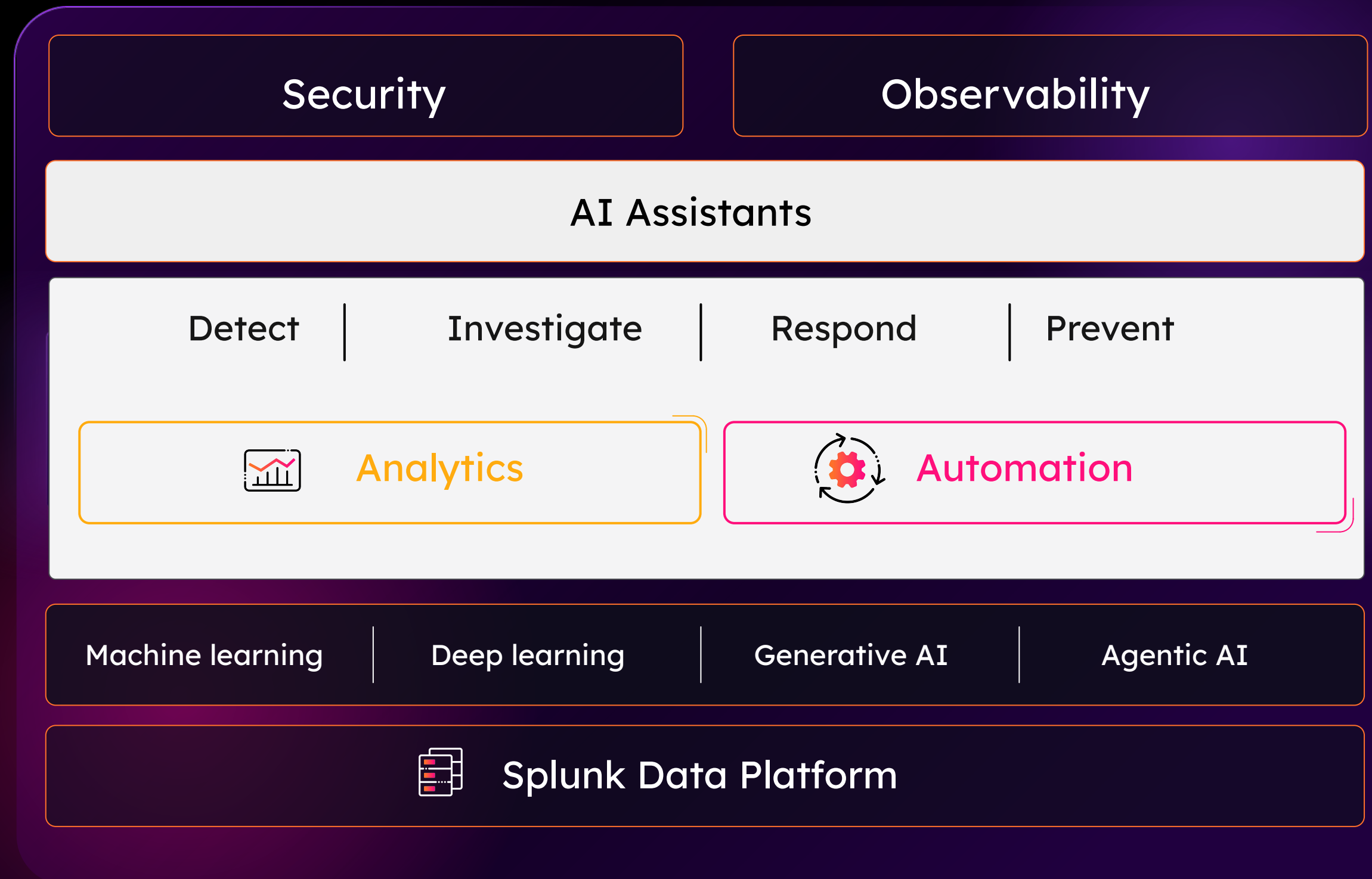
**Splunk  
has been  
innovating  
with **AI**  
since 2015**





# With a foundation of **AI services + data**

- Generative AI Assistants to simplify and make your job easier.
- Prebuilt AI analytics and task automation enabled by agentic AI.
- Powered by leading AI technologies to deliver accuracy and efficiency.
- Integral part of the Splunk portfolio and Data Platform.





# Including a broad portfolio of **ML and AI analytics**



Generative AI

**Make everyone  
an expert**

Reduce need for environment  
and tool expertise by simplifying  
analysis and investigations.



Machine and Deep Learning

**Detect  
and predict**

Real-time,  
streaming analysis  
to detect anomalies  
and forecast trends.

**Correlate  
and diagnose**

Aggregate and analyze all  
data to investigate and  
identify root causes.



# Delivering **productivity increases** when investigating security incidents

Scenario: Security analyst is investigating a high priority RBA finding

## With AI Assistant (in minutes\*)

1. **Summarize findings within an Investigation**
  - a. Leverage Gen AI to generate a summary of findings and relevant MITRE ATT&CK techniques and tactics
2. **Generate SPL queries to investigate data**
  - a. Leverage Gen AI to suggest investigative SPL queries based on natural language prompts
3. **Conversational security inquiries**
  - a. Have security topic related conversations
4. **Generate post-investigation report**
  - a. Leverage Gen AI to create an Investigation Report capturing timeline of events, analyst investigation notes, and MITRE ATT&CK info

## Without AI Assistant (~hours\*)

1. **Review findings**
  - a. Manually review all correlated alerts and metadata to better understand the incident
  - b. Manually research tactics and techniques to better understand the incident
2. **Formulate investigation strategy**
  - a. Leverage tribal knowledge and experience to determine investigation next steps
3. **Broaden the investigation**
  - a. Using tribal knowledge and experience expand the investigation beyond initial findings by manually authoring investigative SPL queries
4. **Post-incident summary report**
  - a. Manually summarize and document initial findings, remediation actions, and other relevant information to close the incident

\*Results will vary depending on complexity of case



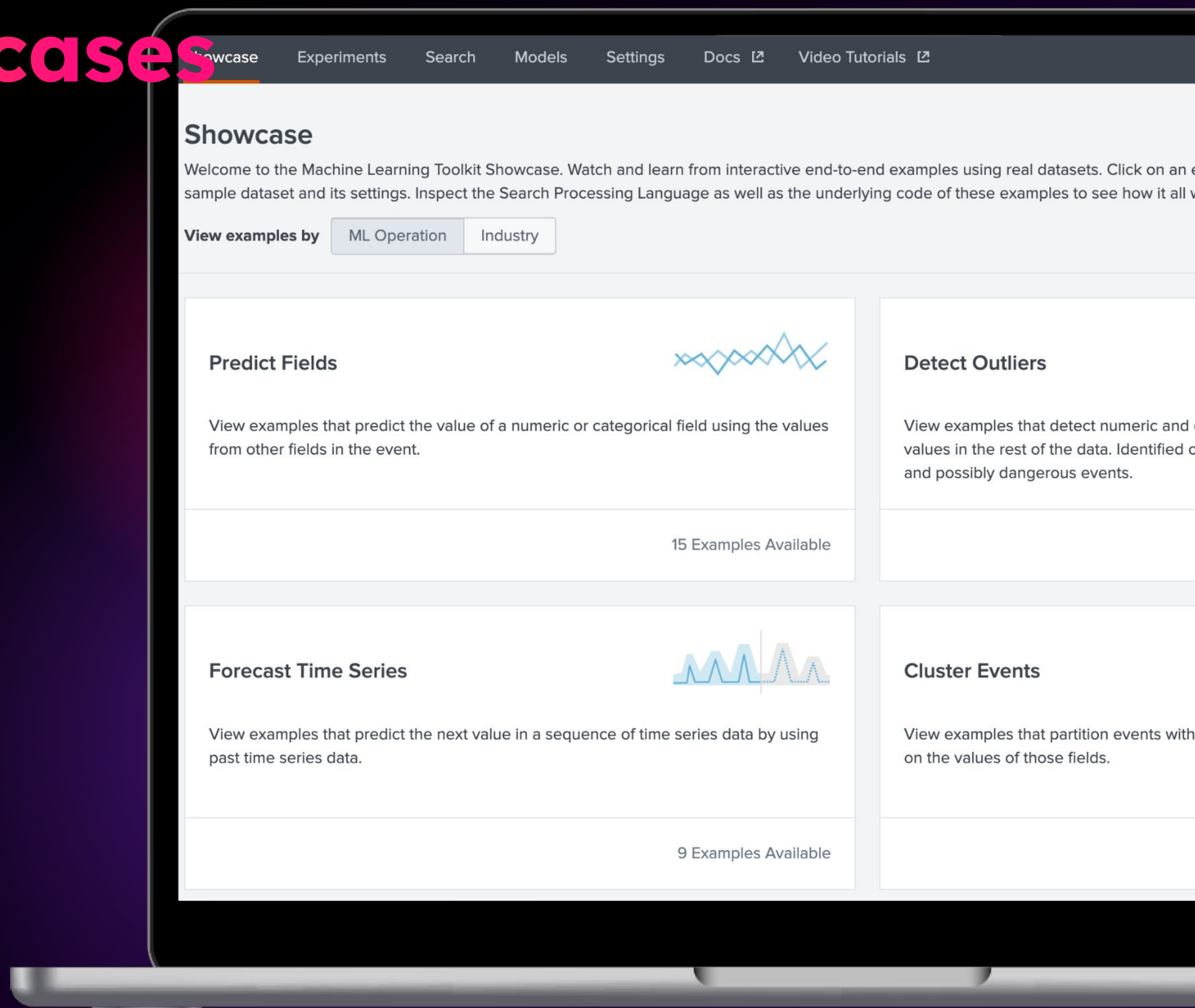
Extend pre-built AI to  
**custom-built AI**



# Customize AI use cases with Machine Learning Toolkit (MLTK)

in Splunk Cloud and Enterprise

- Experiment and model your Splunk data with guided assistant for the whole AI workflow.
- 50+ algorithms to choose from or bring your own model.
- Train and deploy with search commands and operationalize in real-time.

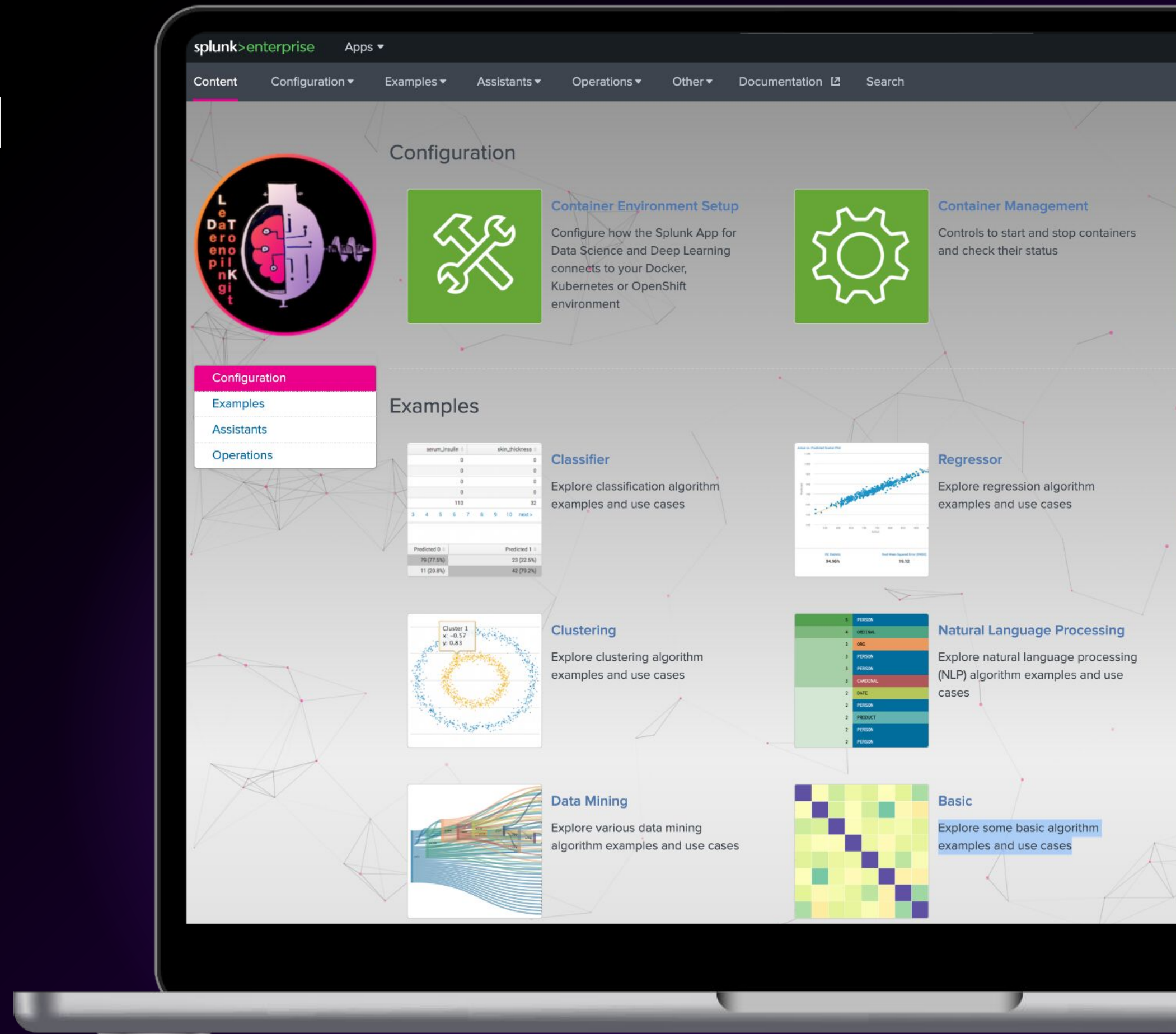




# Extend MLTK to operationalize advanced custom AI/ML use cases

## Splunk App for Data Science and Deep Learning

- **35+ Code Examples:** Guided model building, testing, and deployment
- **Container Management:** productionized for scalability & optimization on CPU & GPU
- State of the art AI frameworks and tools
- Flexible deployments and open source
- Extension to LLMs and VectorDB





# 3. RAG-based LLM Example Dashboard (2)

## Part 2: Querying LLM

LLM-RAG Result

_time ↕	query ↕
2024-06-24 14:27:33	Customer customer@email.com had a Payment processing error during checkout for the product page of DB-SG-G01. Answer the following three questions: 1.Tell me more about this product. 2. List of employees in charge of this product support 3.What were the resolution notes in the past tickets with the same issue description?

LLM Output

RAG\_Response ↕

RAG\_References ↕

User Query:

Customer customer@email.com had a Payment processing error during checkout for the product page of DB-SG-G01. Answer the following questions: 1.Describe this product. 2. List of employees in charge of this product support 3.What were the resolution notes in the past tickets with the same issue description?

I'm happy to help!

\*\*Question 1: Tell me more about this product\*\*

Dragon's Bane - Game of the Year Edition (Xbox Series X) is an immersive fantasy adventure that sets you on a medieval quest. As you explore the world, you'll encounter mythical creatures, engage in dynamic combat, and uncover the secrets of this epic game.

\*\*Question 2: List of employees in charge of this product support\*\*

Buttercup's customer support team for Dragon's Bane - Game of the Year Edition (Xbox Series X) includes:

\* Emily Chen (Senior Customer Support Specialist)

\* Ethan Lee (Customer Support Specialist)

\* Maya Patel (Customer Support Specialist)

\* Julian Sanchez (Customer Support Specialist)

\*\*Question 3: What were the resolution notes in past tickets with the same issue description?\*\*

Although there are no identical issue descriptions, our team has successfully resolved similar payment processing errors in the past. Our typical approach involves:

1. Verifying customer account information and payment details.

2. Troubleshooting potential issues with payment gateways or account validation.

3. Manually processing payments if necessary to complete transactions.

Please note that these answers are based on the limited context information provided and might not be exact or comprehensive.

/srv/notebooks/data/Buttercup/support\_ticket.csv

/srv/notebooks/data/Buttercup/support\_ticket.csv

/srv/notebooks/data/Buttercup/Buttercup\_customer\_support\_list.pdf

/srv/notebooks/data/Buttercup/Buttercup\_customer\_support\_list.pdf

/srv/notebooks/data/Buttercup/Buttercup\_customer\_support\_list.pdf

/srv/notebooks/data/Buttercup/buttercup\_store.xml

/srv/notebooks/data/Buttercup/Buttercup\_Documentation.docx

/srv/notebooks/data/Buttercup/Buttercup\_Documentation.docx

/srv/notebooks/data/Buttercup/Buttercup\_Documentation.docx

Refresh

Refresh Page

Return to Menu

# Thank You

