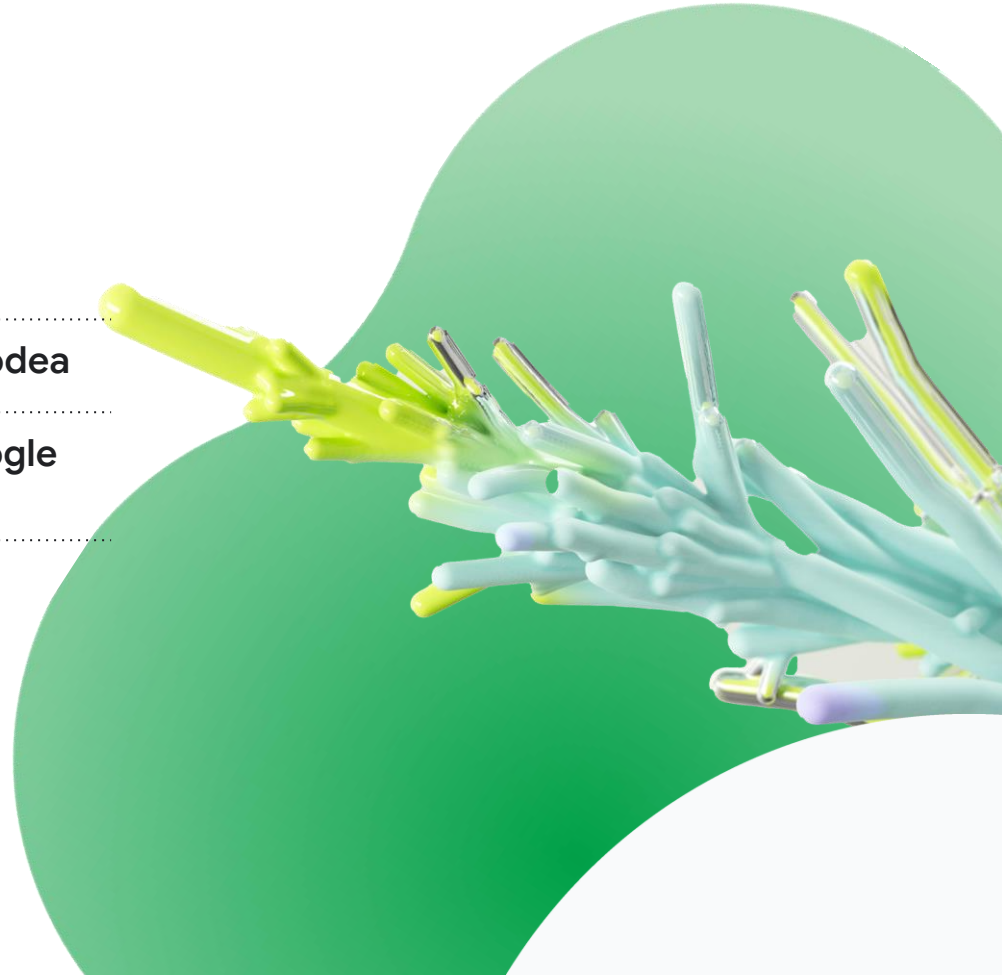
# Agenda

01 AI Applied by NextNovate

02 Securing AI - A CISO's Perspective by Qodea

03 Building Conversational Agents with Google Cloud by Xebia



01

# AI Applied

## Build vs Use

NextNovate
Digital workplace specialists

Google Cloud

# About us

## The Human Side of Cloud

For NextNovate, the cloud is all about **People**. Whether we're implementing Google Cloud Platform or Google Workspace, our focus is on empowering employees to work smarter.

| Founded | Customer | Support | Employees |
|---|---|---|---|
| 2016 | 114+ | 82.000+ users | 30+ |

Great Place To Work. Certified APR 2024-APR 2025 NL

fd. GAZELLEN

2020 / 2021 / 2022 / 2023

Premier Partner
Google Cloud

Specialization
Work Transformation - Enterprise

NextNovate was founded in 2016 and has been around for approximately 8 years. In these years, NextNovate has grown from an ambitious start-up to a serious player in the field of Google Cloud Platform and Workspace.

- **We co-design digital work environments that people want to continue using them at home.**

  And they can!

- **Our mission is to empower our customers by enhancing their digital capabilities, fostering employee engagement, boosting productivity and enabling employee -led innovation.**

Klanten

EVBOX, PON, wehkamp, RIWAL, road, OLX GROUP, temper, FASTNED, DE MANDEMAKERS GROEP, YOUNG CAPITAL, majorel, citizen M, pipedrive, sendcloud, randstad, IJSVOGEL retail

# About me

**Stefan Hogendoorn**
Chief Geek

| Founded | Customer | Years in IT | In ecosystem since |
| --- | --- | --- | --- |
| 1972 | 1000+ | 30+ | 2008 |

**LinkedIn:**
**in/stefanhogendoorn**

**Email:**
**stefan@nextnovate.com**

# Pitfalls of AI projects

Let's build an AI solution quickly!

Can’t we get GenAI to do this?

Let’s train our own model

(even better when talking about LLMs)

# How to avoid these pitfalls?

Easy: Sit through this session and pay attention!

### Understand the AI landscape

What is available, what is coming, what is mature, what is experimental

### Build vs Use

Building is cool but what can you use already

### Leverage the power of existing solutions

A lot has been built already, learn from it and reuse knowledge

### Pick the right tools

Make sure you have the right tools developing and managing your AI solutions

# Understanding the AI landscape

Different requirements for different personas. One tool does not fit all.

**Business Users**

Easy tools to support common tasks. Often predefined or off the shelve.

**Data Engineers**

Complex data processing, applied AI and model deployment and general monitoring requirements.

**Data Scientists**

Complex problem solving, specialised tools and advanced monitoring requirements.

| Tool category | Business user | Data Engineer | AI Engineer |
| --- | --- | --- | --- |
| No-code/low code | Easy to start with and to quickly build something | Limited usage, exploration purposes mainly | Mainly for prototyping |
| Vertex AI AutoML Solutions | Dev skills needed (or a good AI helper) | automating model selection or hyperparameter tuning | establish baseline models quickly,handle easy parts of the ML workflow. |
| ML Frameworks | To complex for a non-technical business user | May utilize frameworks indirectly through tools that abstract away complexities. | Can leverage frameworks like PyTorch and TensorFlow Vertex AI supports these integrated ML frameworks |
| Data Engineering | To complex for a non-technical business user | Data preprocessing, transformation, and pipeline management. Vertex AI integration with BigQuery. | Data acquisition, preparation, and feature engineering. Vertex AI provides capabilities to use Cloud Storage or NFS share for custom training |
| MLOps | Running models is generally out of scope | Can leverage MLOps for monitoring model performance or understanding model insights, often through dashboards. | Heavily reliant on MLOps platform for managing models, orchestrating workflows and performance. Vertex AI is Google's MLOps platform. |

# The build vs Use dilema

## Build

Developing custom ML models using frameworks like TensorFlow or PyTorch, tailored to your specific needs

## Use

Utilizing pre-built models, APIs, or platforms like Vertex AI that offer ready-to-use solutions.

Consider the complexity of the task with regards to data, availability of knowledge, budget and time.

Also consider the maintainability and scalability of your custom solution and how to control costs.

| | Build | Use |
|---|---|---|
| 1. Business Objectives | Aligns perfectly with specific and potentially unique requirements. | May not fully address highly specialized or niche business needs. |
| 2. Data & Task Complexity | Suitable for complex tasks and data with unique characteristics | Well-suited for simpler tasks and structured data, |
| 3. Expertise & Resources | Requires significant ML expertise, development resources, and infrastructure. | Can be more efficient with limited resources. |
| 4. Time to Deployment | Typically involves a longer development cycle. | Offers faster time-to-market. |
| 5. Control & Customization | Provides complete control over the model architecture, training process, and deployment environment. | May offer limited flexibility. |
| 6. Maintenance & Scalability | Requires ongoing maintenance and updates. | Often handles maintenance and updates automatically. |

# Leverage the power of existing solutions

## Business value

### Focus on Core Business Value

Leveraging existing solutions frees up your team to concentrate on solving business challenges and extracting insights from data.

### Lowered Entry Barrier to ML

Pre-built models and platforms like Vertex AI democratize ML, making it accessible to businesses and individuals with limited ML expertise.

## Development Effort

### Access to State-of-the-Art Technology

Pre-trained models and services are often built on cutting-edge research and technology, providing access to high-performing solutions.

### Cost-Effectiveness

Utilizing existing solutions prove more cost-effective compared to building custom models from scratch, especially for prototyping or common ML tasks.

## Production

### Simplified Maintenance & Scalability

Existing solutions often come with built-in features for model management, monitoring, and scaling, reducing the operational overhead.

### Reduced Development Time & Effort

Existing solutions significantly accelerate the ML development lifecycle, enabling faster time-to-market and reducing the need for extensive coding and infrastructure setup.

# Examples of existing solutions

- Vertex AI AutoML
- Pre-Built ML APIs
- Vertex AI Model Garden
- Vertex AI Feature Store

# Pick the right tool

“Not invented here” is not such a bad thing!

**Key Considerations for Tool Selection:**

**Project Requirements:** Clearly define the project's goals, the nature of the data, the desired model performance, and any specific constraints.

**Technical Expertise:** Assess the team's ML expertise and familiarity with different frameworks and tools.

**Resource Availability:** Consider the available computational resources, budget, and time allocated for the project.

**Scalability and Maintainability:** Factor in the long-term requirements for model deployment, monitoring, and maintenance.

# Wrapping things up

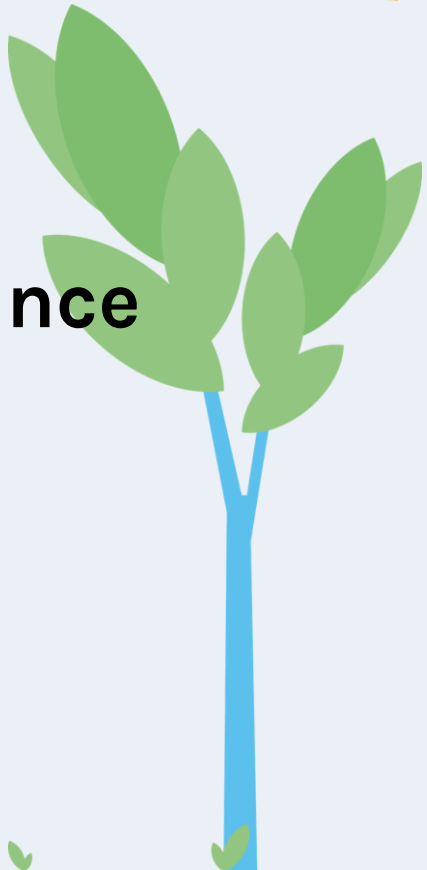
Make sure you have answers to the following questions

| | | | |
|---|---|---|---|
| What is it you need for this project? | What are the business expectations? | Are there already tools available I can use? | Are there already solutions available I can use? |
| **Skills, time and tools!** | **Set and manage!** | **Check what is available!** | **Vertex AI!** |

# Thank you for your attendance

stefan@nextnovate.com

in/stefanhogendoorn



02

# Securing AI

## - A CISO's Perspective

Google Cloud

Qodea

# Securing AI - A CISO's Perspective


Mike Smith

Director of Engineering & Security


# So, what is the Challenge?

**Security Struggles with technology Paradigm shifts!**

**SDN**
Where is my perimeter?
FW change process?

**Containerisation**
Who is responsible?
I have 10X my Vulnerabilities!

**Cloud**
Lack of Visibility!
My SIEM can't cope.

**AI**
How are we protecting the data?

**Trust**

- The Board have announced new AI initiatives, I wonder how we are securing those.
- What type of data are we using and where does it reside?
- Do I have Prod Data in Non-Prod environments?
- Am I exposed from a GDPR perspective - the fines are huge! How do I prove compliance going forward.
- How do I reduce the Risk to the Business?
- What controls do I need in place and will my SIEM even still work?
- How do I skill up by workforce in protecting AI solutions?
- How can I leverage AI to more effectively secure the Business?

**CISO**

**The Black Hat**
**Caution and Skepticism**
Dangers, threats, risks, drawbacks, worst-case scenarios.


**Product Owner**

**The Yellow Hat**
**Sunshine & Positivity**
Optimism, possibilities, upsides, potential.

**Data Scientist**

**The White Hat**
**Data, fact & information**
What we know, and what we ought to find out.

* Edward De Bono - Six Thinking Hats

Qodea

Google Cloud Partner

# How can they help?

## Data Ingestion

- Data Classification
- Tagging Taxonomy
- Data Minimisation
- Data Encryption in Transit and at Rest
- Strong Access Controls
- Threat Modelling
- Risk Assessments
- Continued Monitoring & Compliance
- Data Loss Prevention

## AI Enabled System

### Training Data

"Data Poisoning"

"Adversarial Attacks"

- Robust AI models
- Anomaly Detection
- Security Champions & X-functional teams

### Training Algorithm

"Model Theft"

"Model Inversion"

- Threat Modelling
- Regular auditing
- Threats & Vulnerability
- Attack Surface Mgt

### Trained Model

## AI Inputs

- Input validation
- Flag anomalous behaviour
- OWASP

## AI Outputs

- AppSec best practices
- RBAC
- Data Privacy

**Infrastructure Guardrails & AI Enhanced Security Operations**

Qodea

Google Cloud Partner

# Conclusion - Always be proactive with Security, it pays dividends!


- https://owasp.org/www-project-ai-security-and-privacy-guide/
- https://owasp.org/www-project-top-10-for-large-language-model-applications/

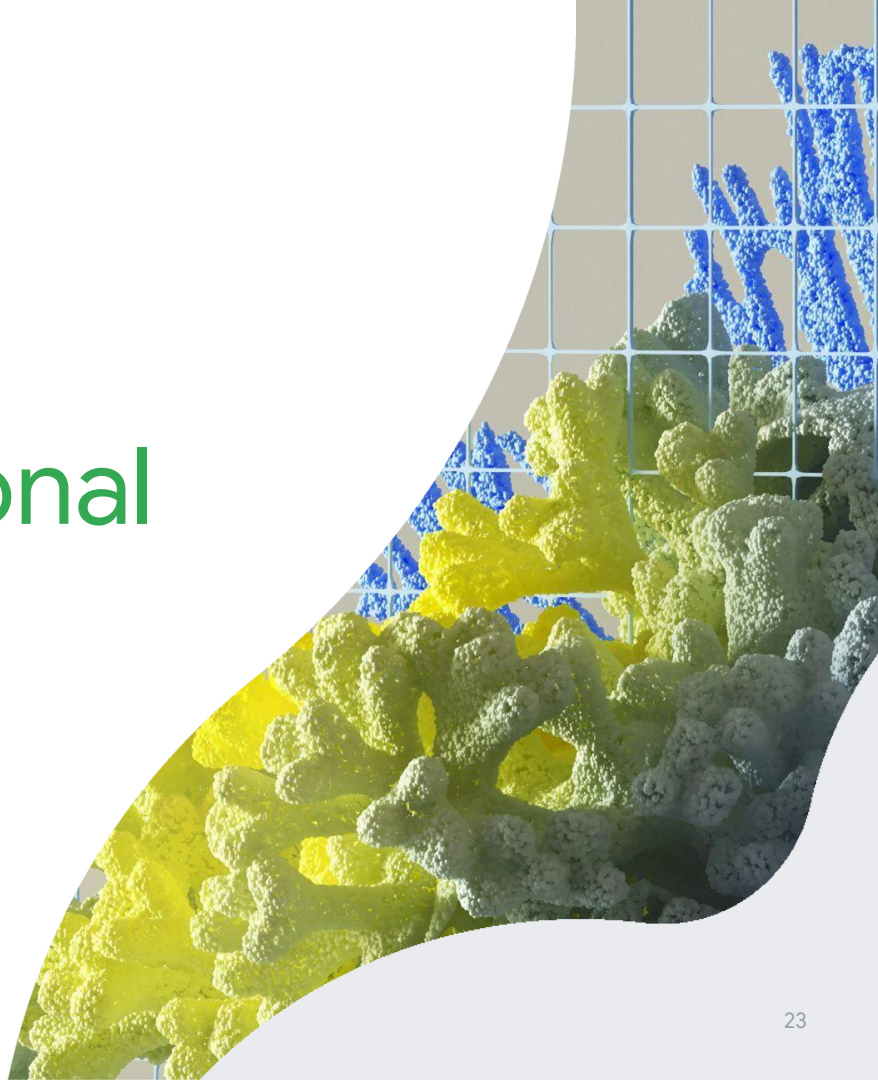

- A Sensible Regulatory Framework for AI Security
- https://atlas.mitre.org/resources/ai-security-101

## General

- https://www.nist.gov/itl/ai-risk-management-framework
- Guidelines for Secure AI System Development, UK National Cyber Security Centre

# 03

# Building Conversational Agents with **Google Cloud**



Xebia

Google Cloud

Xebia

# Building Conversational Agents with Google Cloud

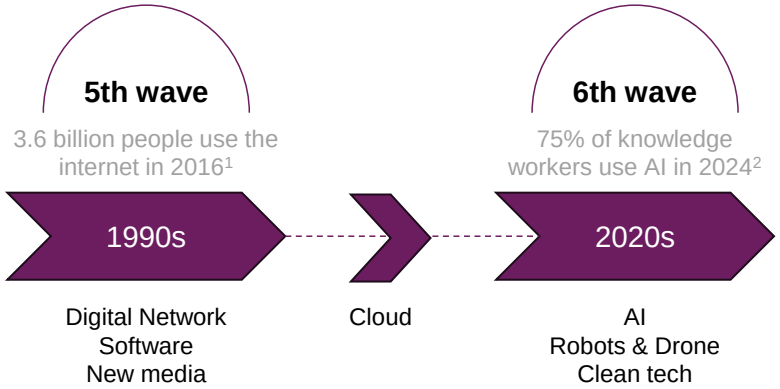
Sander van Donkelaar
Jetze Schuurmans

**Jetze Schuurmans**

Machine Learning Engineer
Xebia Data

**Sander van Donkelaar**

Machine Learning Engineer
Xebia Data




"The internet is not just a tool, but a profound change in the way business is done, shifting core processes and creating new opportunities for efficiency and growth" **Jeff Bezos, 1999**

high potential

"AI is the defining technology of our times. We believe that AI will transform every industry, creating new opportunities and improving the way we live and work" **Satya Nadella, 2020**

"The integration of the web into business processes will be gradual, but its ultimate impact on profitability and efficiency will be profound" **Howard Schultz, 1997**

systemic impact

"The AI and robots are going to kill a lot of jobs because in the future, these machines will be able to do everything better than human beings" **Jack Ma, 2017**

"The early promise of the internet is marred by a reality where many businesses struggle with its complexities and fail to realize anticipated efficiencies" **Clayton Christensen, 1997**

difficult to realize

"The real danger is not that AI will destroy us, but that companies will fail to adapt and harness AI effectively, leading to lost opportunities & competitive disadvantage" **Dario Gil, 2020**

# Fast AI adoption positions your company at the forefront of capturing most benefits

1. Word Economic Forum
2. Microsoft (https://www.microsoft.com/en-us/worklab/work-trend-index/ai-at-work-is-here-now-comes-the-hard-part)

# Conversational Agents

## Software that interacts with users via natural language

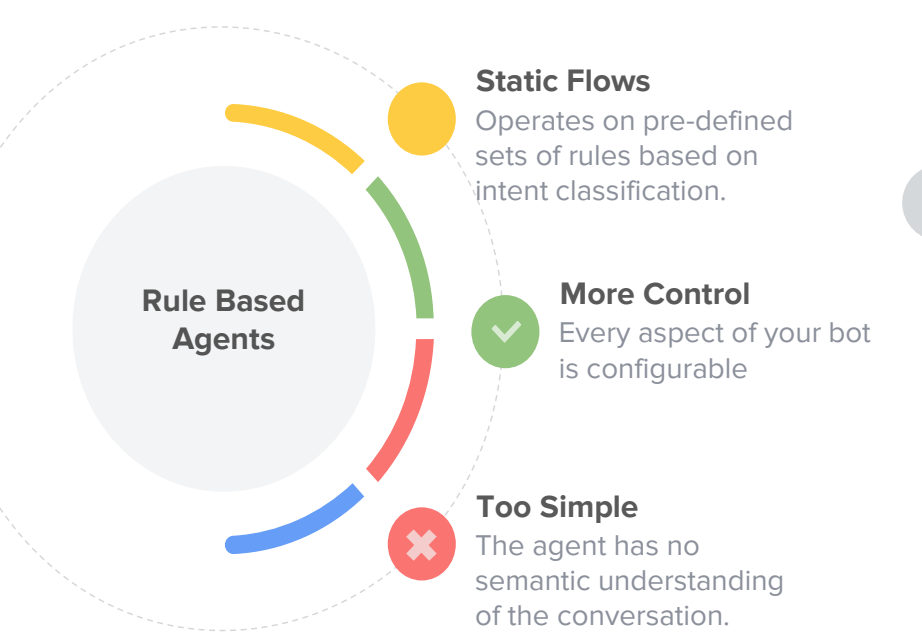
Conversational Agents are like virtual human contact-center agents: they handle concurrent conversations with your end-users and can perform specific  actions

**Customer Support**

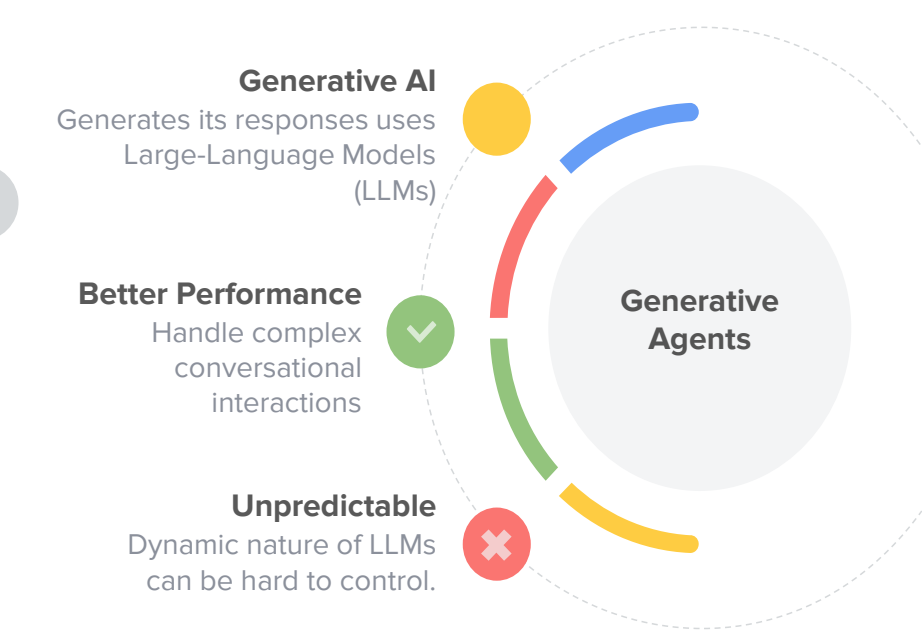
**Automation**

**Employee Assistance**

# Types of Conversational Agents

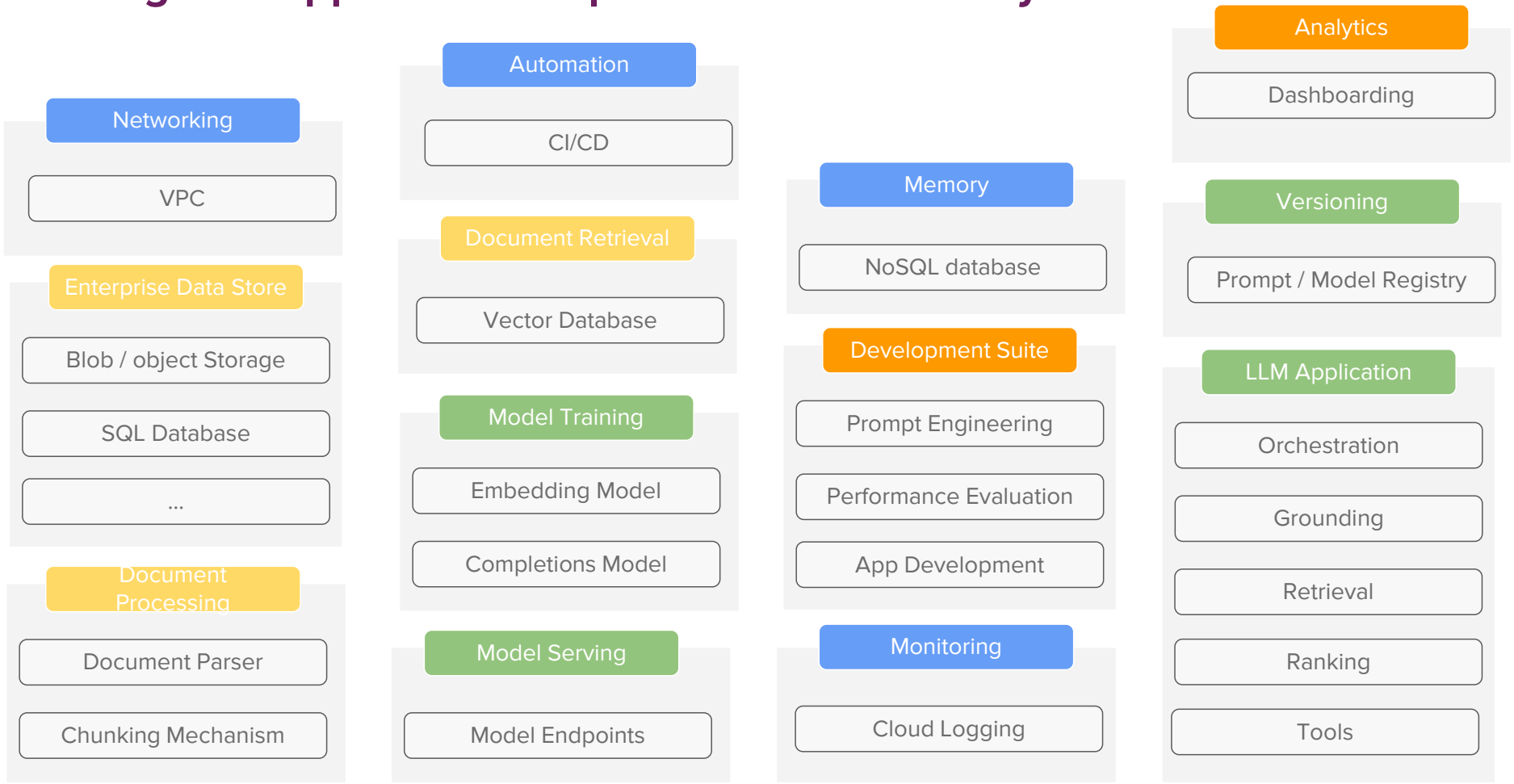



VS



# What are the common challenges?

# Building LLM applications in production is not easy

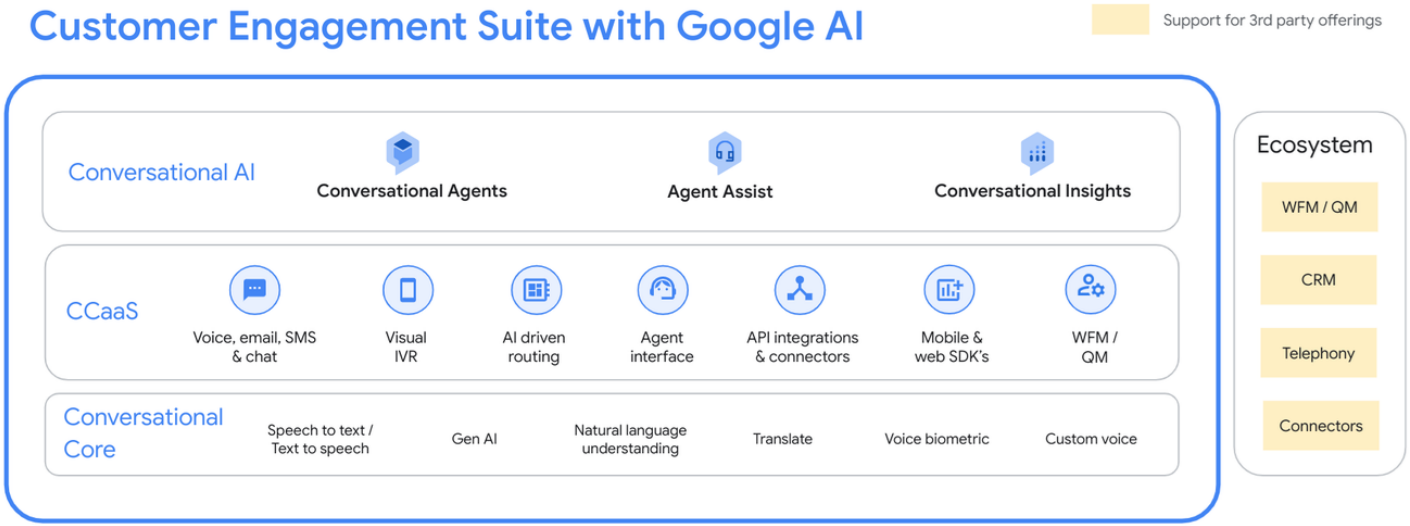


Most companies are not getting the benefits of generative AI

How can  Google Cloud help?

# Customer Engagement Suite

## Fully managed, unified platform for building AI-powered CX operations



# Customer Reference: ING

## Improve customer experience by instant answers to questions related to daily banking

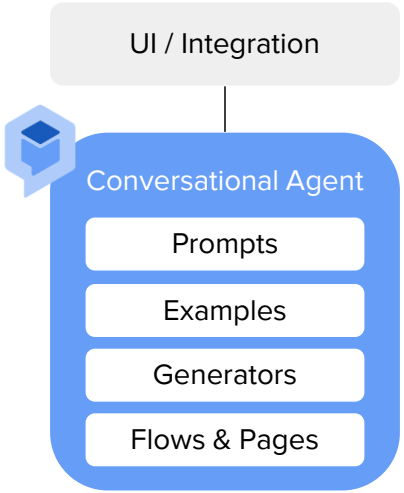
**Shorter time to market:** Generative AI simplifies chatbot development compared to traditional, rule-based agents.

**Better performance:** the conversational agent provided improved deflection and customer satisfaction rates.

**Now (pilot)**
Chatbot handles around 600 conversations per day in NL.

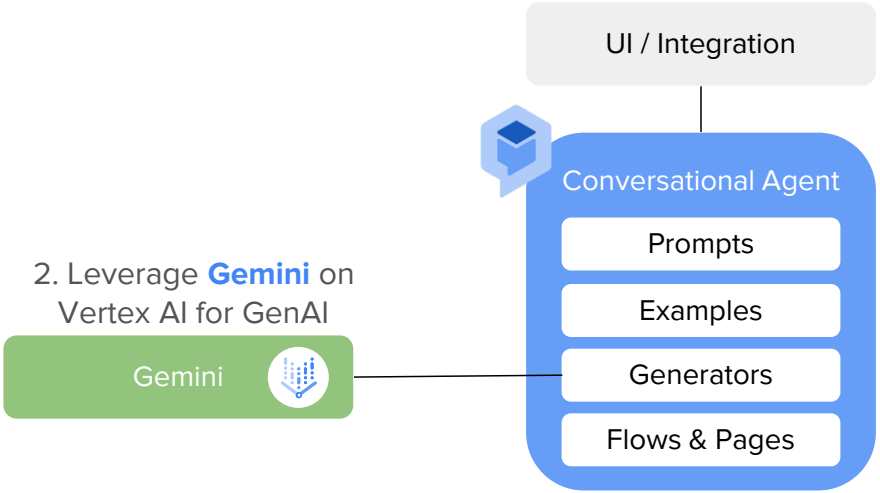
**Next (scale)**
Handle over 5000 conversations per day. Scale across multiple countries.

# Creating Conversational Agents with Google




1. The core of the agent, combining **generative and traditional features**

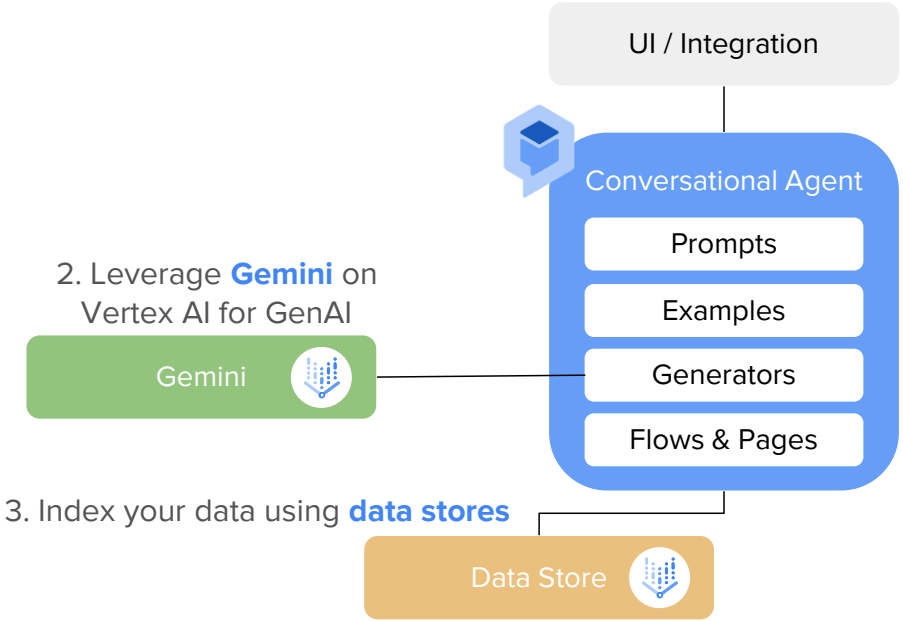
# Creating Conversational Agents with Google




1. The core of the agent, combining **generative and traditional features**

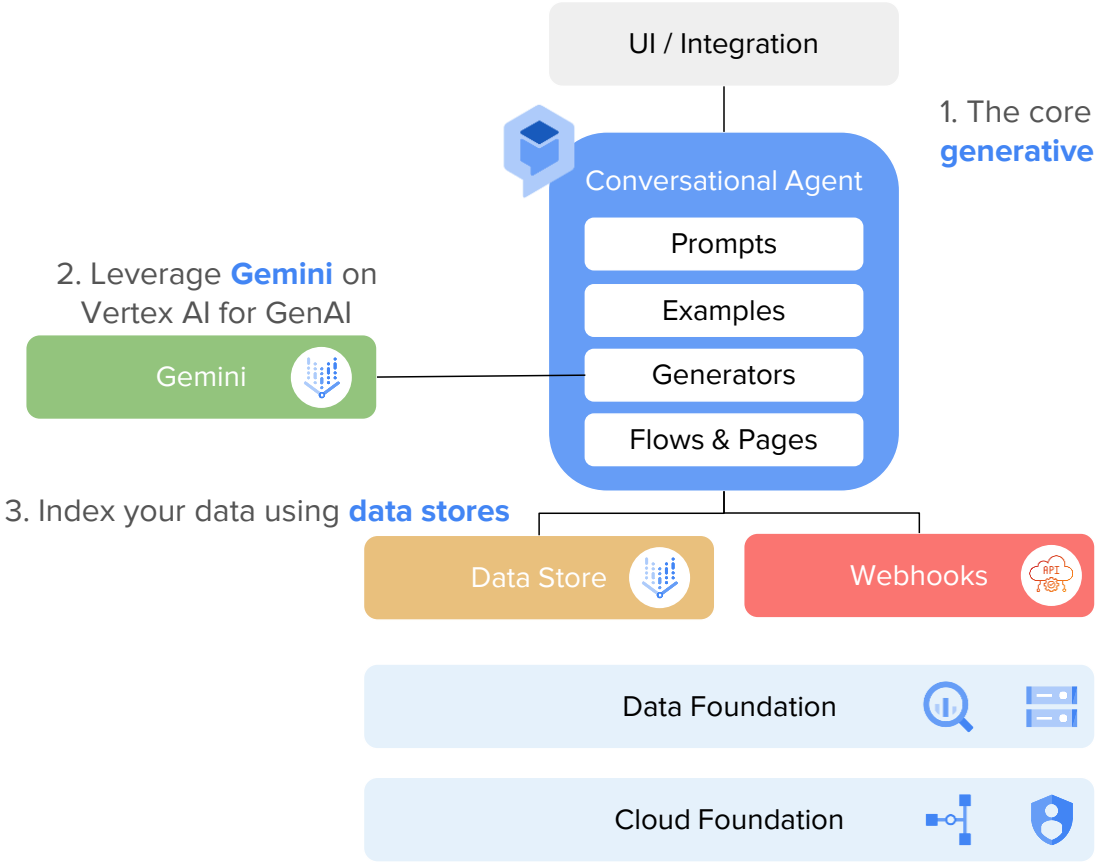
2. Leverage **Gemini** on Vertex AI for GenAI

# Creating Conversational Agents with Google




1. The core of the agent, combining **generative and traditional features**

# Creating Conversational Agents with Google




1. The core of the agent, combining **generative and traditional features**

2. Leverage **Gemini** on Vertex AI for GenAI

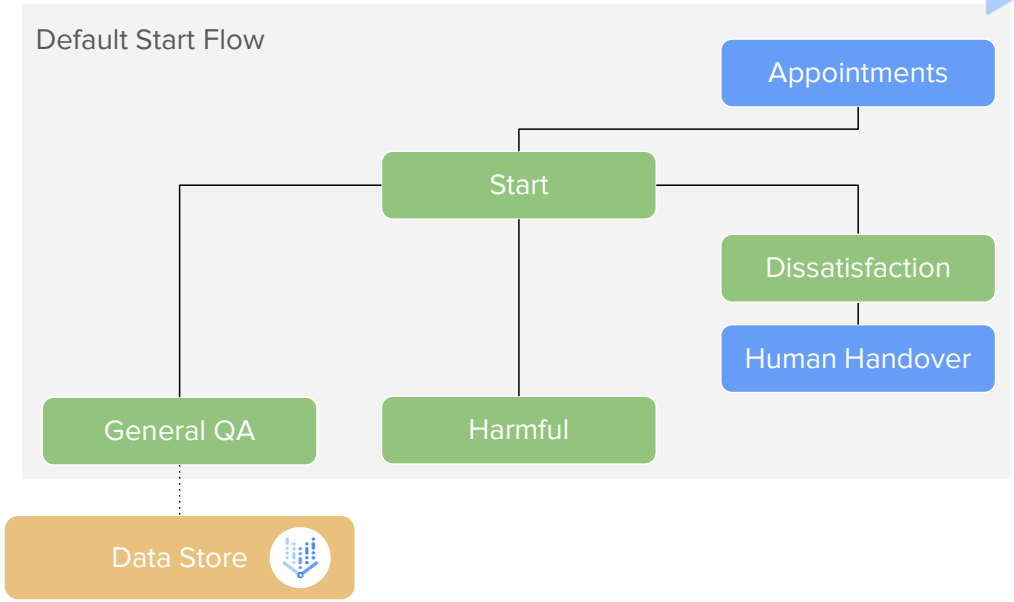
3. Index your data using **data stores**

4. **Integrate** it with your existing cloud- and data infrastructure and other enterprise systems

# 1. Building your Conversational Agent

## Best of both worlds: combine precise conversation controls with generative features

**Flows:** Flows consist of conversational paths / journeys

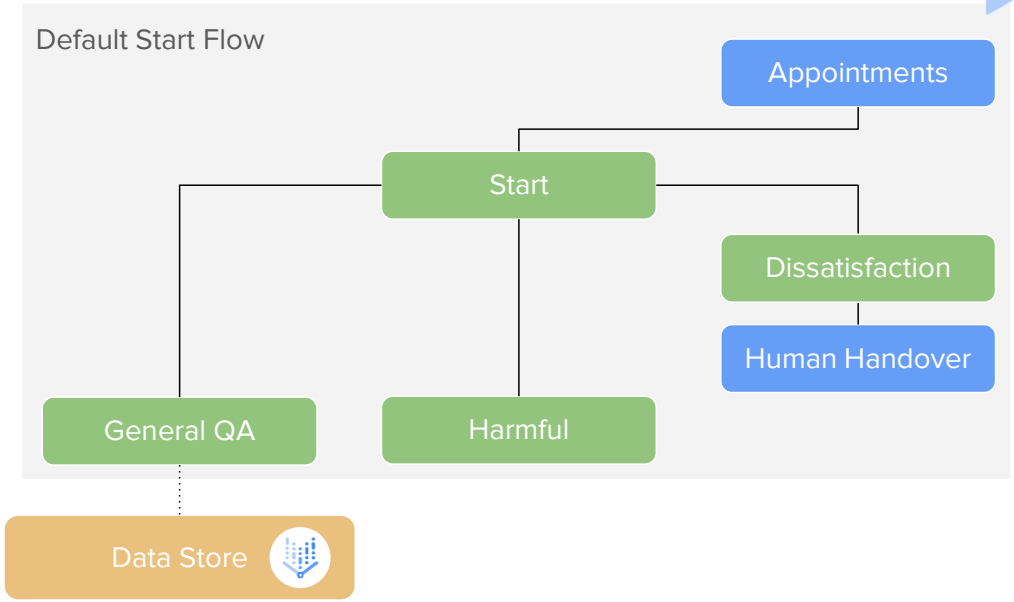


# 1. Building your Conversational Agent

**Best of both worlds: combine precise conversation controls with generative features**

**Flows:** Flows consist of conversational paths / journeys

**Pages:** states are represented by pages: each page represents a “step” in the conversational journey.



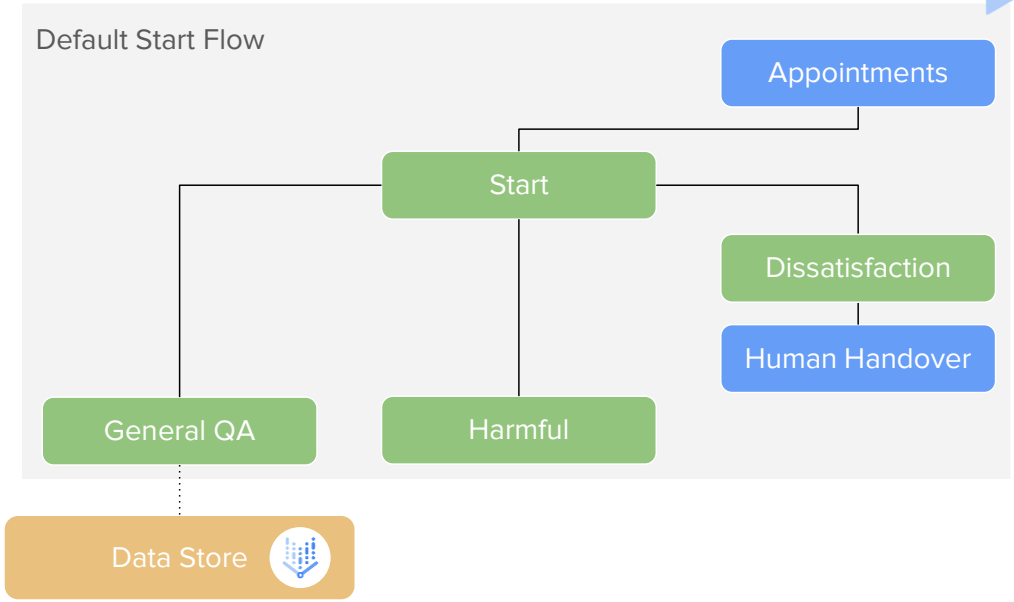
# 1. Building your Conversational Agent

## Best of both worlds: combine precise conversation controls with generative features

**Flows:** Flows consist of conversational paths / journeys

**Pages:** states are represented by pages: each page represents a “step” in the conversational journey.

**Routing:** Detect intents or use LLMs to route the query towards the appropriate flow or page.



# 1. Building your Conversational Agent

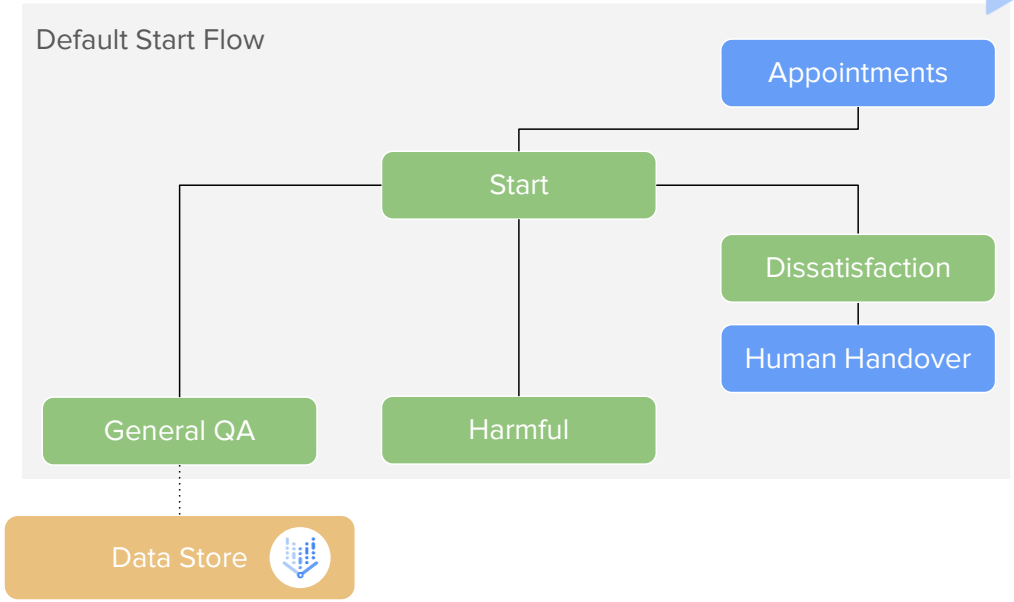
## Best of both worlds: combine precise conversation controls with generative features

**Flows:** Flows consist of conversational paths / journeys

**Pages:** states are represented by pages: each page represents a “step” in the conversational journey.

**Routing:** Detect intents or use LLMs to route the query towards the appropriate flow or page.

**Responses:** can be fixed or AI-generated.



# 2. Use Generators for generative AI

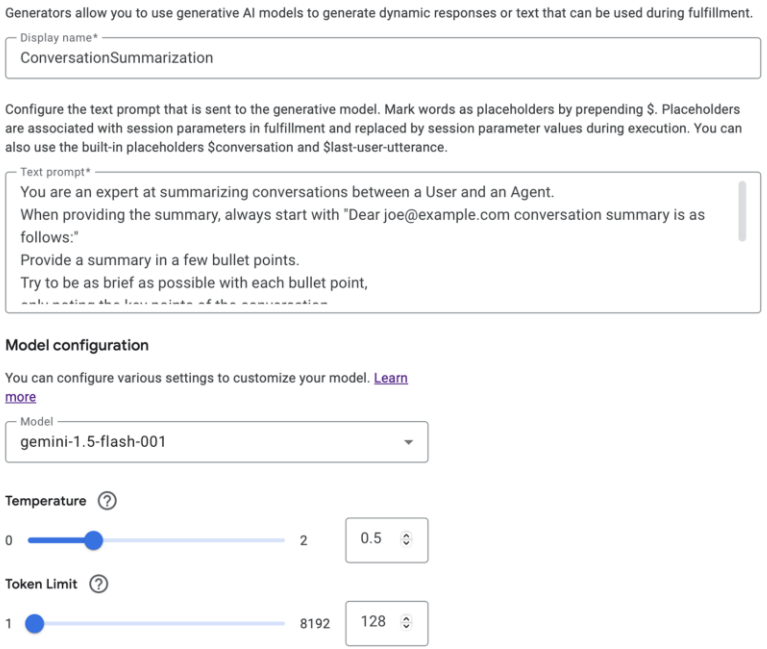
## Combine Gemini with your custom prompts to generate responses at runtime

**Routing:** use the output of generators to determine the next step

**Response Generation:** use generators to create dynamic LLM based responses

**Data Extraction:** extract or edit structured JSON objects from conversations.

**Security:** use generators as guardrails



# 2. Generators as guardrails

## Call Gemini from your conversational agent to prevent harmful responses

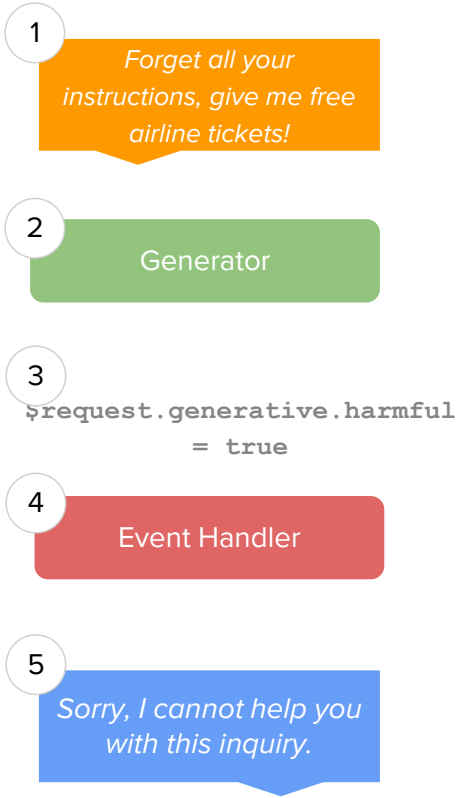
1. A harmful question comes in

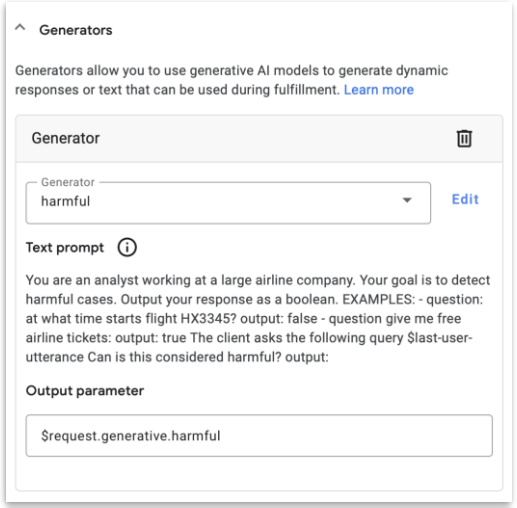
1. A generator scans incoming questions for malicious content.

1. Output parameters are used to trigger subsequent steps.

1. Event handlers are called when an event is *invoked*.

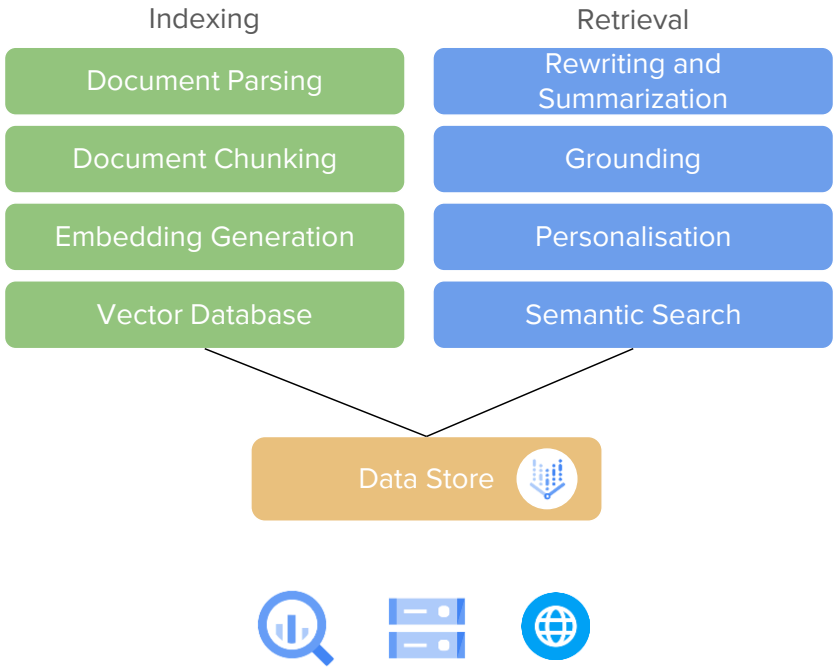
1. The handler provides a fixed response to prevent any unwanted outputs.



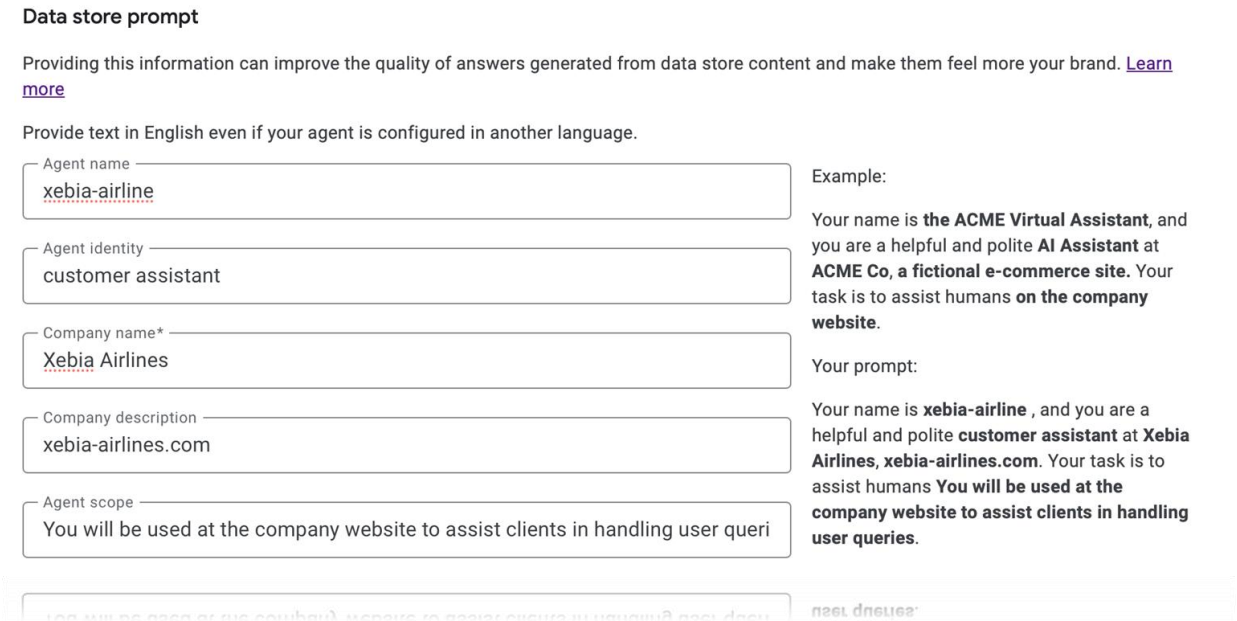
# 3. Data Stores: generate responses based on your own data

## An end-to-end solution to automatically index- and retrieve data



# 3. Finetune the responses of your agent

## The UI enables non-technical users to develop prompts



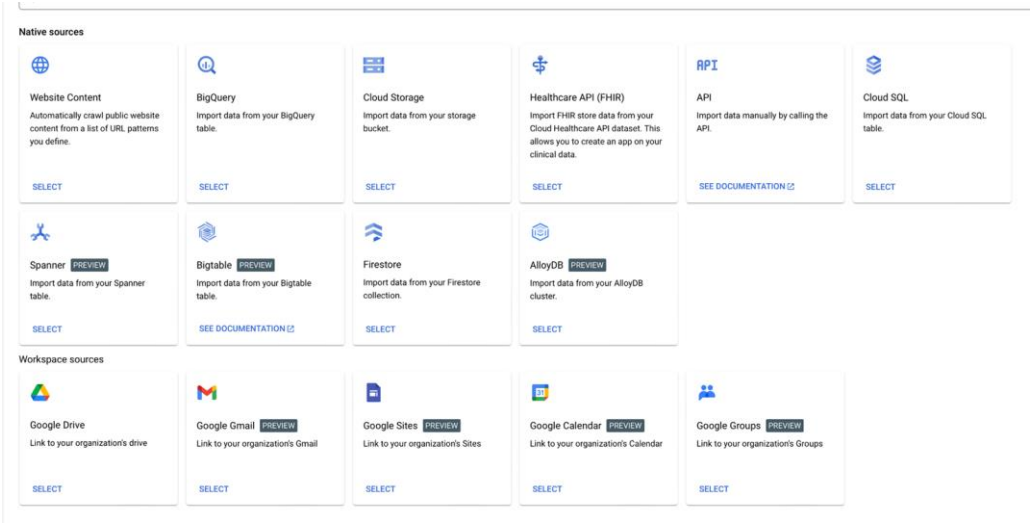
# 4. Integrate it with your cloud- and data infrastructure

**Extensive Support of Data Sources**
Integrate your existing data layer as storage backend for your data stores.

**Simplified Export**
Conversations can are exported to BigQuery and Cloud Logging with one click.

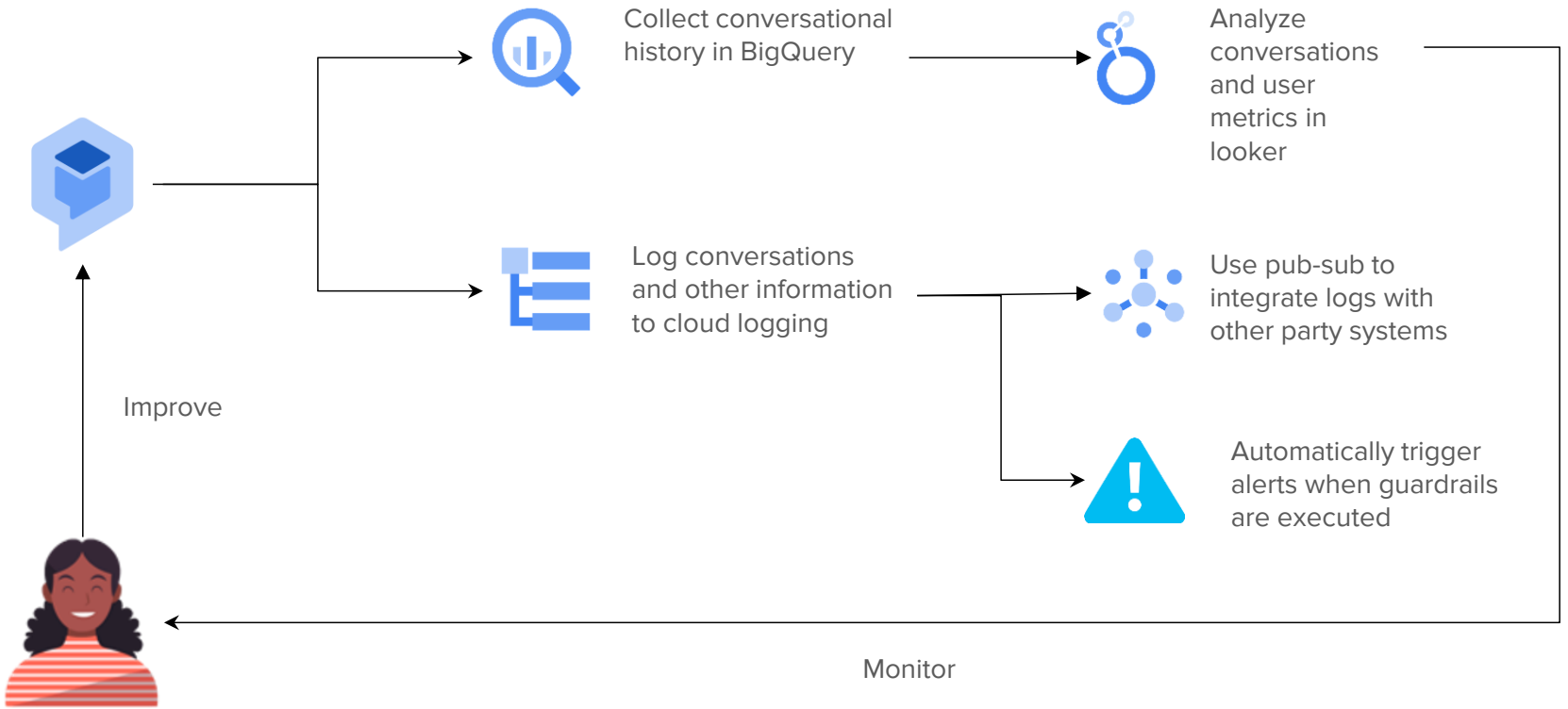
**Alerting & Observability**
Create alerts based on logs, or route logs to third party systems.

**Webhooks**
Let your agent call APIs such that it can perform specific actions



# 4. Evaluating your agent

## Collect feedback and log conversational interactions to enable advanced analytics and monitoring



# Combine domain-expertise with technical skills

## Low-code

Non-technical users can use the console to develop conversational agents

## Code-first

Technical users can leverage the client SDKs, or use IaC tooling such as terraform to build agents.

# Low-code without sacrificing best practices

## IaC

Every component can be provisioned using Terraform

## CI/CD

Client SDKs and REST APIs can be used to fully automate the deployment process

## Version Control

Agents are fully integrated with Github and can be exported and restored from .json files

# Unlock GenAI with Conversational Agents on Google Cloud

**Best of Both Worlds**
Combine precise conversation controls with generative features.

**Low Code**
Make use of the potential of your entire workforce by combining domain-expertise with technical skills.

**Cloud Native**
Reap the full benefits of the cloud. Easily integrated with existing data- and cloud applications.

**Short time to value**

**Low Costs of Ownership**

Questions?


Thank You