Transformation you can *trust*.

How Pega Blueprint securely manages **data, privacy, and AI.**

Pega Blueprint™ Security & Privacy

Pega Blueprint™

Security & Privacy Summary

We built Pega GenAI Blueprint™ with your privacy and security as priorities. We understand your processes aren't just diagrams and workflows – they're your competitive advantage.

Access managed by your enterprise

Blueprint access can be connected to your enterprise single-sign on.

- Blueprint manages data access through role-based access control to ensure the Blueprints created remain private to the creator unless actively shared.
- When a user leaves your organization, they will lose access to your Blueprints when their status or roles are updated in your organizations SSO provider.

No AI is trained on your Blueprints

Prompts, data, and designs are never fed into AI models for training.

- Blueprint leverages multiple LLMs under the hood – including Anthropic models on AWS, Google Gemini, and OpenAI on MS Azure.
- All LLM's are continually governed, performance tested and leverage provider best practices for content filtering.

Data remains confidential

The details of your Blueprints are stored in an encrypted cloud database.

- Deployed in the cloud in the region which makes most sense for your business – US, UK, APAC, or EU.
- No data shared across Pega clients or partners.
- Blueprints remain private to the creator unless actively shared.
- Only activity-level reporting data leveraged within Pega by authorized personnel (email address, create time, create name)

Enterprise-grade cloud security

Your Blueprint data gets the same rock-solid protection as our production Pega Cloud Environment including:

- 256-bit AES encryption for data at rest and HTTPS/TLS protection for data in transit.
- Continuous monitoring with host-based virus protection and intrusion prevention systems.
- State-of-the-art operations centers that take physical and environmental security seriously.
- Built-in safeguards against DDoS attacks and automatic blocking of known malicious IP addresses.

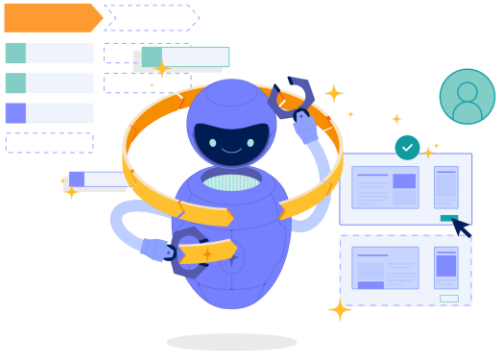
01

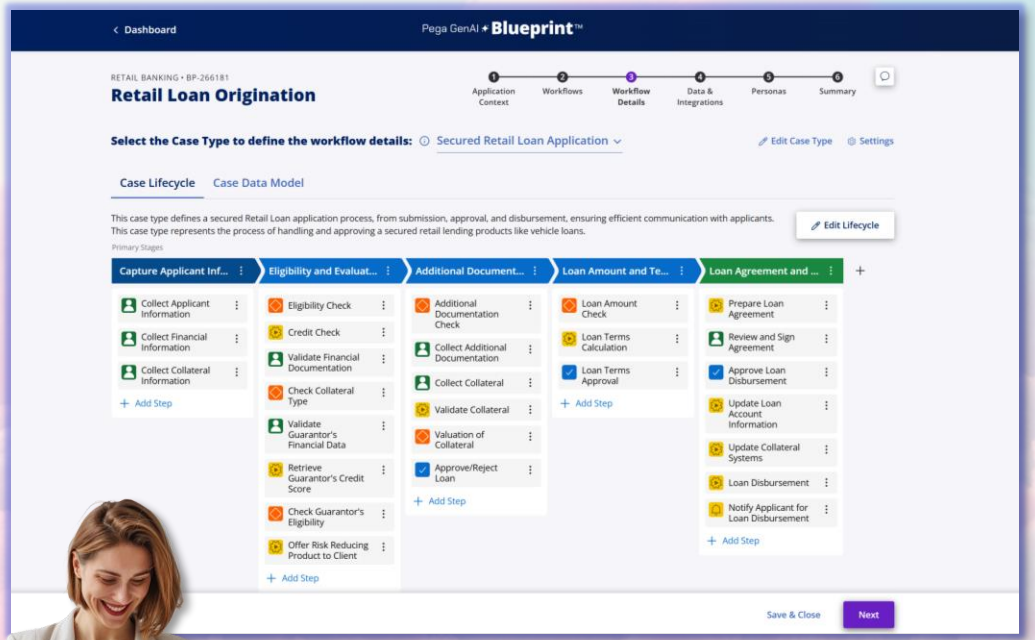
What is Pega Blueprint?

PEGA BLUEPRINT™

Transformation rocket fuel

Pega Blueprint is enterprise workflow development powered by AI. Focused on bringing people & AI together to accelerate automation & jumpstart transformation.





Where does Blueprint fit in the SDLC?

Rapid design to jumpstart development

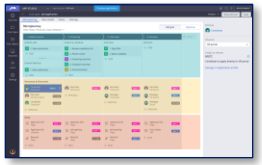
Design → Build → Test & deploy → Operate → Optimize

Pega Blueprint™

Business & IT collaboration to accelerate initial workflow design with GenAI.

No PII *

Operated securely by Pega Cloud®

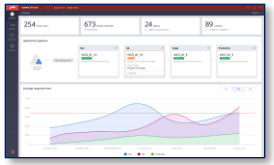


Pega Infinity™
Pega App Studio

Deep configuration of integration, automation, etc. to turn Blueprints into complete apps

No PII *

Private client deployment

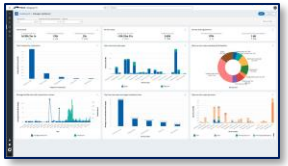


Pega Infinity™
Pega Deployment Manager

Automated DevOps pipelines orchestrating route-to-live, including tests, approvals, security scans, and more

No PII*

Private client deployment



Pega Infinity™
-

Secure end-user experiences to access workflows (locked down through role & access based controls)

Potentially sensitive

Private client deployment

Pega Infinity™
Pega Process Mining

Analyze workflows to uncover process gaps & inefficiencies

Potentially sensitive

Operated securely by Pega Cloud®

*Based on design time use cases, it is not advised to manage PII at these phases

02

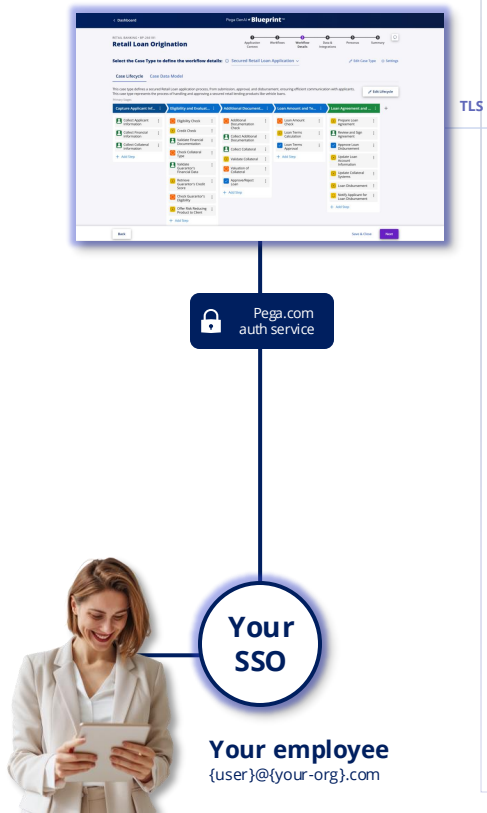
Blueprint architecture.

Pega Blueprint™ Architecture

Blueprint runs securely in Pega Cloud® on AWS – managed & operated following leading cloud standards.

High level architecture:

- Blueprint authentication connects to your enterprise single-sign on protocol (SSO).
- Pega offers geographically segmented data residency services specific to its Pega Cloud offering. Blueprint geographic region is based on your enterprise location (within either US, UK, European Union, Australia, Singapore, or Japan.).
- Blueprint processing runs on a secure, reliable Pega Infinity application, fully backed by the operational strength of Pega Cloud services, delivering enterprise grade reliability, compliance, security, & disaster recovery.
- Blueprint leverages LLM's based on use case & performance. Primarily Claude models running on AWS Bedrock.
- No AI is trained on your Blueprint data.
- Blueprint data is encrypted in transit with TLS.
- Blueprint data is securely stored & encrypted at rest.



Pega Blueprint™ Regional Data Residency (EU, UK, US)

Enterprises located in the

European Union

- Storage & compute: **AWS EU-Central (Frankfurt)**
- AI Model Execution

	Provider	Model / provider	LLM regions
aws	**AWS Bedrock** Primary provider	Anthropic	AWS Bedrock: European Union
	Google Cloud	Gemini	Google Vertex: European Union
	Microsoft Azure	OpenAI GPT	Microsoft Azure: European Union

Enterprises located in the

United Kingdom

- Storage & compute: **AWS EU-Central (Frankfurt)**
- AI Model Execution

	Provider	Model / provider	LLM regions
aws	**AWS Bedrock** Primary provider	Anthropic	AWS Bedrock: European Union
	Google Cloud	Gemini	Google Vertex: European Union
	Microsoft Azure	OpenAI GPT	Microsoft: European Union

Enterprises located

Across the globe

- Storage & compute: **AWS US-East**
- AI Model Execution

	Provider	Model / provider	LLM regions
aws	**AWS Bedrock** Primary provider	Anthropic	AWS Bedrock: United States
	Google Cloud	Gemini	Google Vertex: United States
	Microsoft Azure	OpenAI GPT	Microsoft Azure: United States

For Pega Partners

Define which enterprise you're creating a Blueprint on behalf of in the organization name field on the functional description page of blueprint and those Blueprints will be stored & managed within region on behalf of that enterprise, automatically.

Determining which region a Blueprint is stored within

Check out the Blueprint ID – which will have a regional identifier if it is stored & managed within the EU, AU, UK, JP, or SG.

Pega Blueprint™ Regional Data Residency (APAC)

Enterprises located in the

Australia

- Storage & compute: **AWS: Australia - Sydney**
- AI Model Execution

	Provider	Model / provider	LLM regions
aws	**AWS Bedrock** Primary provider	Anthropic	AWS Bedrock: Australia
	Google Cloud	Gemini	Google Vertex: Australia
	Microsoft Azure	OpenAI GPT	Microsoft Azure: Australia

Enterprises located in the

Japan

- Storage & compute: **AWS: Japan - Osaka**
- AI Model Execution

	Provider	Model / provider	LLM regions
aws	**AWS Bedrock** Primary provider	Anthropic	AWS Bedrock: Japan/APAC
	Google Cloud	Gemini	Google Vertex: Japan
	Microsoft Azure	OpenAI GPT	Microsoft Azure: Japan / European Union

Enterprises located

Singapore

- Storage & compute: **AWS: Singapore**
- AI Model Execution

	Provider	Model / provider	LLM regions
aws	**AWS Bedrock** Primary provider	Anthropic	AWS Bedrock: APAC
	Google Cloud	Gemini	Google Vertex: Singapore
	Microsoft Azure	OpenAI GPT	Microsoft Azure: European Union

For Pega Partners

Define which enterprise you're creating a Blueprint on behalf of in the organization name field on the functional description page of blueprint and those Blueprints will be stored & managed within region on behalf of that enterprise, automatically.

Determining which region a Blueprint is stored within

Check out the Blueprint ID – which will have a regional identifier if it is stored & managed within the EU, AU, UK, JP, or SG.

03

Access & authentication.

Pega Blueprint™ Access & Auth

Set up access to Blueprint with your single-sign on (SSO).

Enabling users to authenticate against your Organization's IDP ensures that only authorized users are accessing ALL Pega sites and applications, such as Blueprint, My Support Portal, etc.

When Federated Authentication is enabled, at log in, users will not be prompted to provide a password and will be redirected to authenticate against their Identity Provider.

IT leads at the client Organization can work with our integrated account team to enable Federated Authentication.

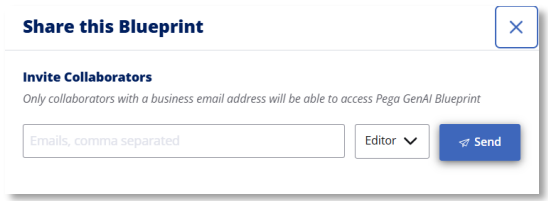
What we need from you: **SAML 2.0 Configuration details** or **OAuth Configuration details**

Login to following applications will use Federated authentication: Blueprint, Pega.com, community.pega.com, academy.pega.com, support.pega.com, docs.pega.com, partners.pega.com, saleshub.pega.com, partner-logo-generator.pega.com, My Support Portal, My Pega Cloud, My Pega, PDC, Deployment Manager, Pega Trials

Blueprints are only visible to the creator, unless actively shared.

By default, Blueprints are not visible to anyone beyond the user who created them (the Blueprint *owner*).**

Blueprint owners have the ability to share the Blueprint with additional stakeholders (e.g. teammates, partners, etc.). They can invite users via email as either *editors* or *viewers*.



When a user leaves your org, their Blueprints don't leave with them.

If an enterprise has federated their SSO with Pega digital properties (e.g. Blueprint), only users with active access to their SSO will be able to log into Blueprint.

If a user changes the domain registered with their pega.com profile – for example switches organizations, the Blueprints that they created within their old domain will no longer be visible.

Access to those Blueprints can be restored for other users within the organization upon request.

**Visible only to authorized Pega administrative Cloud Operations personnel.

04

Data privacy.

Pega Blueprint™ Data Handling

What's captured & how is it handled?

#	Datapoint	Format	Processed by LLM?	Used for AI Training?	Stored in...	Visible to...
1	**Creator information**	Metadata (name, email, org)	No	No	**Pega Cloud Data Storage** Fully encrypted*	Pega
2	**App description**	Metadata (industry, app name)	Yes – to inform initial Blueprint template	No	**Pega Cloud Data Storage** Fully encrypted*	Pega
3	**Text based application description**	Encrypted text	Yes – to inform initial Blueprint template	No	**Pega Cloud Data Storage** Fully encrypted*	Only Blueprint creator & invitees**
4	**Legacy documentation**	.PDF, .DOC, .DOCX	Yes – to inform initial Blueprint template	No	**Pega Cloud File Storage** Encrypted at rest*	Only Blueprint creator & invitees**
5	**Legacy videos & images**	.MOV, .MP4, .JPG, .PNG	Yes – to inform initial Blueprint template	No	**Pega Cloud File Storage** Encrypted at rest*	Only Blueprint creator & invitees**
6	**Process diagrams**	.BPMN	Yes – to inform initial Blueprint template	No	**Pega Cloud File Storage** Encrypted at rest*	Only Blueprint creator & invitees**
7	**Integration & data documentation**	.YAML, .SQL, .DDL, .CRD	Yes – to inform initial Blueprint template	No	**Pega Cloud File Storage** Encrypted at rest*	Only Blueprint creator & invitees**
8	**Blueprint edits & final designs**	Encrypted metadata (exported as encrypted .Blueprint file)	No	No	**Pega Cloud Data Storage** Fully encrypted*	Only Blueprint creator & invitees**

*Blueprint data can be permanently deleted upon request through Pega Support.
**Visible only to authorized Pega administrative Cloud Operations personnel.

05

Cloud security.

Visit the Pega Cloud Trust Center to learn more

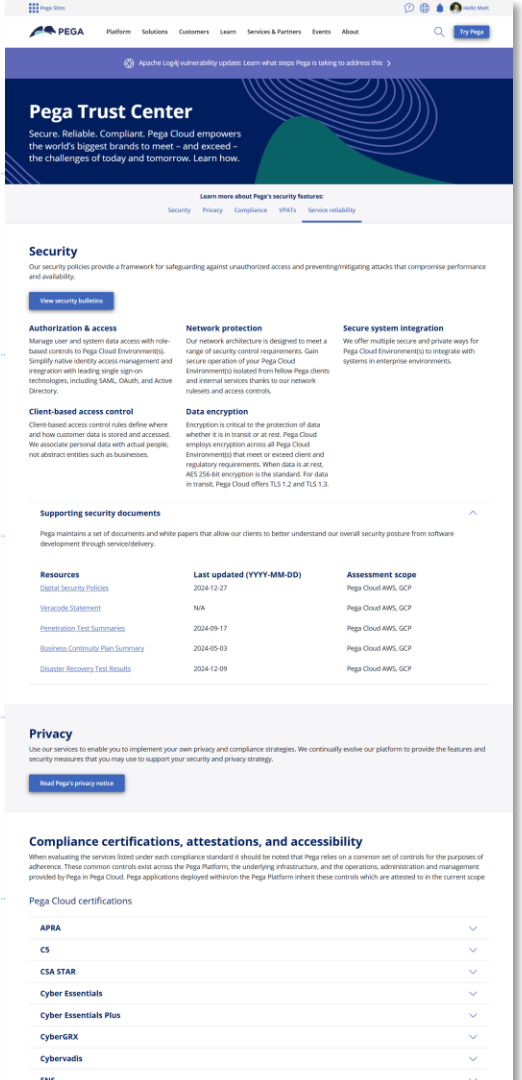
Pega Blueprint™ Cloud Security

Pega Blueprint runs on Pega's proven Pega Cloud® services, ensuring enterprise-grade security.

Transformation you can rely on.

- 24/7 operations monitoring, management, and support
- Secure-by-design architecture operations with strict access controls and operational safeguards-minimizing human touch through automation
- Enterprise-grade compliance, uptime, disaster recovery, and threat modeling

Operations	**24/7 monitoring, environment support, & proactive response** Details
Access	**Environment governed by automated operational controls and strict access protocols** Details
Compliance	**Strict adherence to 20+ industry standards** Details
Disaster recovery	**Comprehensive data & service back-up, failover, restoration** Details
Threat modeling	**Follow red team methodology based on OWASP top 10** Details
Availability	**Architecture leverages built-in high availability and disaster recovery to support near continuous uptime.** Details



06

AI governance.

Pega Blueprint™ leverages a mix of frontier models to help drive rapid transformation

Models are all securely managed & incorporated into the product to balance effectiveness & performance.

As of Q3 2025

While Pega continually assesses LLM's to ensure we're using the right model for the right job, here are models currently utilized under the hood:

	Hyperscaler	LLM Provider	Blueprint region	LLM region
aws	**AWS** Primary provider	Anthropic	AMS (USA)	AWS Bedrock: United States
			EU	AWS Bedrock: European Union
			UK	AWS Bedrock: United Kingdom
	Google Cloud	Google Gemini	AMS (USA)	Google Vertex: United States
			EU	Google Vertex: European Union
			UK	Google Vertex: United Kingdom
	Microsoft Azure	OpenAI - GPT	AMS (USA)	Microsoft Azure: United States
			EU	Microsoft Azure: European Union
			UK	Microsoft Azure: United Kingdom

All agreements with hyperscalers include commitments that no prompts or data sent by Pega or clients will be accessed by either the hyperscaler or the LLM provider.

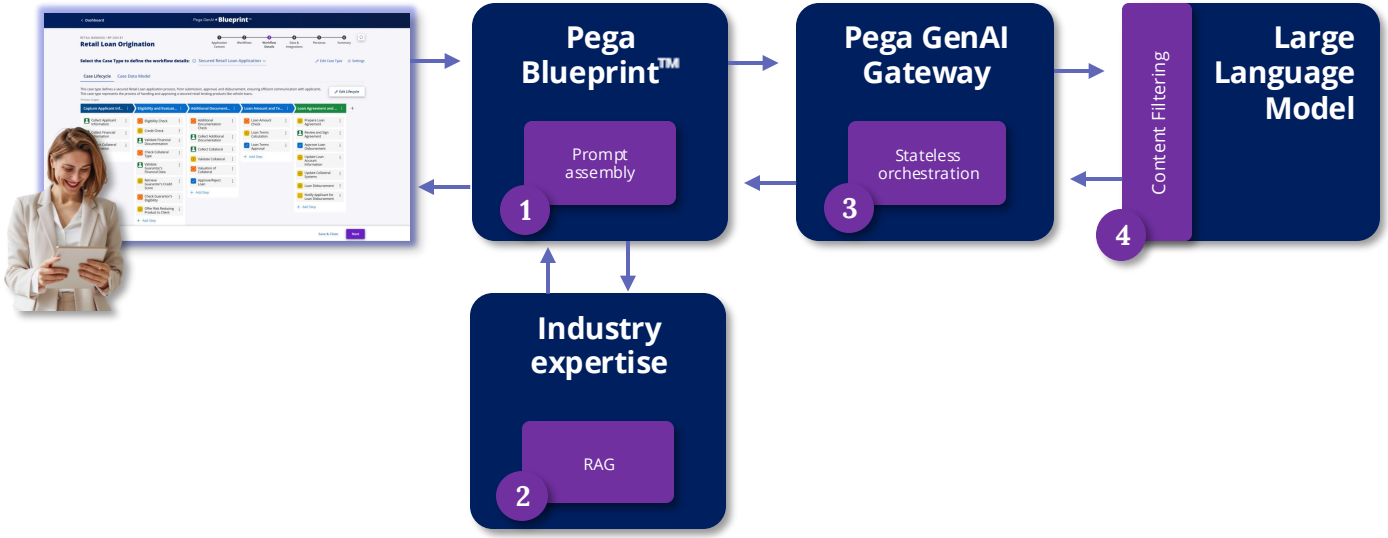
*as of June 2025
**Always up-to-date on pega.com

AI Data Flow

Pega Blueprint™

Secure, safe AI handling:

1. Pega Blueprint **creates prompts** that describe the application based on user-entered information.
2. Pega Blueprint calls out to Pega's **industry expertise** knowledgebase run on Pega Knowledge Buddy to synthesize industry best practices based on Blueprinted use case and enrich LLM prompts & Blueprint creation.
3. All LLM calls are brokered by the **Pega GenAI Gateway Service** on Pega Cloud. This service provides a trusted layer of security, segmentation, and scalability for communication with large language providers.
4. When sending an encrypted prompt to a secure LLM, **content filtering** applies to detect and prevent harmful content in prompts and completions.



Content filtering approach

Pega relies on the most proven Large Language Model Providers in its delivery of Pega capabilities that rely on Generative AI. Within each model, are robust content filtering capabilities that will mitigate the possibilities of harmful, unethical, or toxic responses from occurring. While the capabilities are robust, these are only mitigations and the possibility for a jailbreak remains. In addition, each model provider takes a different approach to achieving the same outcome of responsible and ethical AI.

This means that the dassification models, thresholds, and categories of detection can differ. When different models are used different content classification and filtering is applied. When clients are using Pega GenAI Connect, they should be aware of these possible differences and perform testing to validate them.

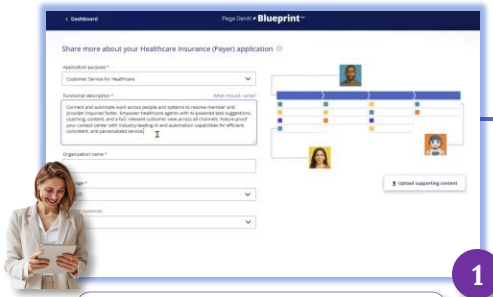
AI Data Flow

Pega Blueprint™

Content filtering approach

Pega relies on the most proven Large Language Model Providers in its delivery of Pega capabilities that rely on Generative AI. Within each model, are robust content filtering capabilities that will mitigate the possibilities of harmful, unethical, or toxic responses from occurring. While the capabilities are robust, these are only mitigations and the possibility for a jailbreak remains. In addition, each model providers take a different approach to achieving the same outcome of responsible and ethical AI.

This means that the classification models, thresholds, and categories of detection can differ. When different models are used different content classification and filtering is applied. When clients are using Pega GenAI Connect, they should be aware of these possible differences and perform testing to validate them.



1

Clients initiate a blueprint design session by giving a functional description of the solution they envision.

Pega assembles a set of prompts using the functional description enriched by our industry expertise buddies, as well as the interpretation of client uploaded documents and send this towards the LLM

Pega Blueprint™

Prompt assembly

2

Industry Expertise

RAG

Pega Knowledge Only

3

Pega applies decades of industry expertise in the vertical and use case selected to enrich the functional description

Pega GenAI Gateway

Stateless orchestration

4

All LLM calls are brokered by the **Pega GenAI Gateway Service** on Pega Cloud. This service provides a trusted layer of security, segmentation, and scalability for communication with large language providers.

Content Filtering

Large Language Model

6

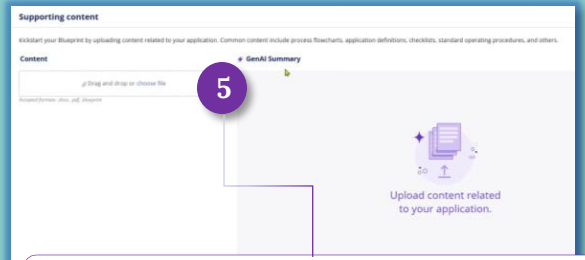
When sending a prompt to a public LLM, **content filtering** applies to detect and prevent harmful content in prompts and completions.

Blueprint Case

Document Interpretation

Cloud File Storage

Document Stored

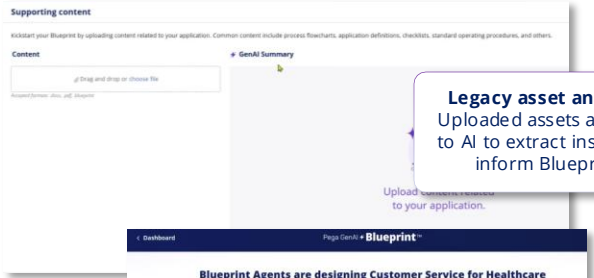


5

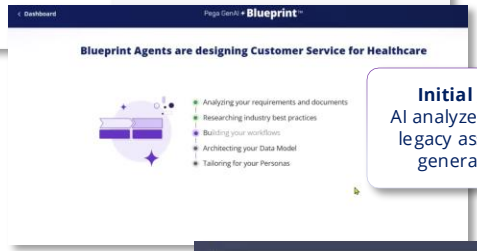
Optionally, clients upload relevant documentation such as flow charts, checklists, or standard operating procedures that define the current process they are looking to automate.

AI Data Flow

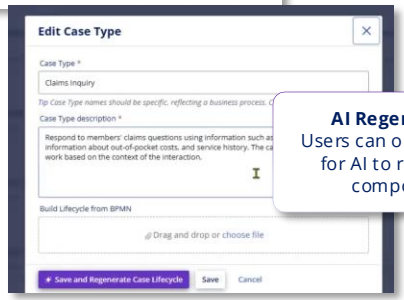
Pega Blueprint™



Legacy asset analysis
Uploaded assets are sent to AI to extract insights & inform Blueprint



Initial generation
AI analyzes description & legacy asset analysis to generate Blueprint



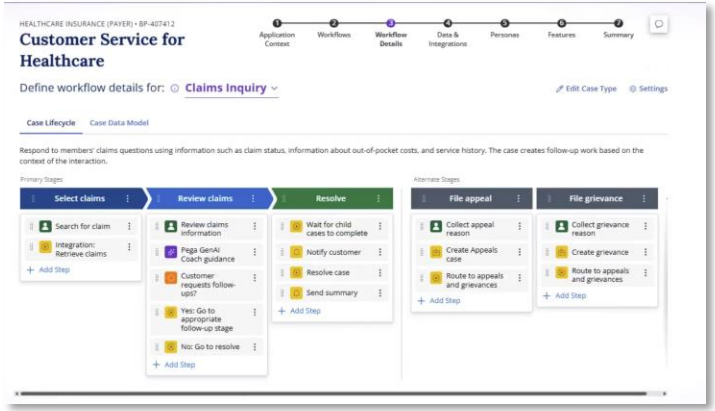
AI Regeneration
Users can optionally ask for AI to regenerate components

Pega GenAI Gateway

Stateless orchestration

Content Filtering

Large Language Model



AI Governance at Pega

End-to-end oversight

Pega's AI Governance board is run by the Cloud Security team and oversees all AI utilization across Pega's products.

It brings together experts & owners from Product, Cloud Security, Cloud Operations, IT, Legal, & Go-to-market to ensure all utilization of AI in Pega is safe, responsible, secure.

Strategic Partnerships

In order to deliver on the unique needs of its enterprise clients, Pega has formed strategic relationships & overarching agreements with AWS, Google Cloud, and Microsoft to drive shared AI initiatives.

Pega & its cloud providers of LLM services meet regularly to review model options, performance, security, & issues.

Security-first

Pega's AI Governance board organizes & executes continuous security assessments of all AI powered capabilities including Pega Blueprint.

Security assessments run include:

1. ISO 42001
2. Microsoft AI Red Team Methodology
3. OpenAI Safety Best Practices
4. Microsoft required mitigations
5. OWASP Top 10 for LLM Applications
6. OWASP Cloud-Native Application Security Top 10

Pega is the leading Enterprise Transformation Company™ that helps organizations Build for Change® with enterprise AI decisioning and workflow automation. Many of the world's most influential businesses rely on our platform to solve their most pressing challenges, from personalizing engagement to automating service to streamlining operations. Since 1983, we've built our scalable and flexible architecture to help enterprises meet today's customer demands while continuously transforming for tomorrow. For more information on Pega (NASDAQ: PEGA), visit http://www.pega.com