



Transformation you can *trust*.

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

— Pega Blueprint™ Security & Privacy



Dashboard Pega GenAI • **Blueprint™**

Application Context Workflows Workflows Details

RETAIL BANKING • BP-206191

Retail Loan Origination

Select the Case Type to define the workflow details: ☐ Secured Retail Loan Application

Case Lifecycle Case Data Model

This case type defines a secured Retail Loan application process, from submission, approval, and disbursement, ensuring efficient communication with applicants. This case type represents the process of handling and approving a secured retail lending products like vehicle loans.

Primary Steps

Capture Applicant Inf...	Eligibility and Evaluat...	Additional Document...	Loan Amount and Te...	Loan Agreement and ...
<ul style="list-style-type: none">Collect Applicant InformationCollect Financial InformationCollect Collateral Information + Add Step	<ul style="list-style-type: none">Eligibility CheckCredit CheckValidate Financial DocumentationCheck Collateral TypeValidate Guarantor's Financial DataRetrieve Guarantor's Credit ScoreCheck Guarantor's EligibilityOffer Risk Reducing Product to Client + Add Step	<ul style="list-style-type: none">Additional Documentation CheckCollect Additional DocumentationCollect CollateralValidate CollateralValuation of CollateralApprove/Reject Loan + Add Step	<ul style="list-style-type: none">Loan Amount CheckLoan Terms CalculationLoan Terms Approval + Add Step	<ul style="list-style-type: none">Prepare Loan AgreementReview and Sign AgreementApprove Loan DisbursementUpdate Loan Account InformationUpdate Collateral SystemsLoan DisbursementNotify Applicant for Loan Disbursement + Add Step

[Save & Close](#) [Next](#)

Table of contents



01 What is Pega Blueprint?

Users
Operating model
Business value

02 Blueprint architecture.

Cloud architecture
Deployment regions

03 Access & authentication.

User management
Single-sign on (SSO)
Permissions

04 Data privacy.

Data flow
Storage & encryption
Visibility & access

05 Cloud security.

Operations
Threat modeling
Disaster recovery

06 AI governance.

LLM utilization
Risk & controls
LLM governance

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 organization's 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, 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.



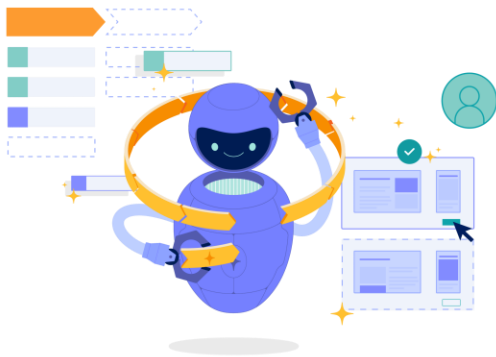
01

What is Pega Blueprint?



Transformation rocket fuel

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




How does it work?



#1

Accelerate legacy analysis.

Rather than manually analyzing legacy systems, **extract insights automatically** by uploading:

- **Documentation** (e.g. SOP)
- **Source code** analysis
- **Videos** & screens

#3

Collaborate seamlessly.

Blueprint is 100% collaborative add all **business & IT collaborators** to:

- **Rapidly adapt** AI suggestions
- Capture requirements in **common language**
- **Preview app** throughout

#2

Build on best practices.

Based on requirements, AI Agents behind Blueprint **compose a starting point application** informed by:

- **Industry** best practices
- Pega & partner **expertise**
- Organizational **knowledge**

#4

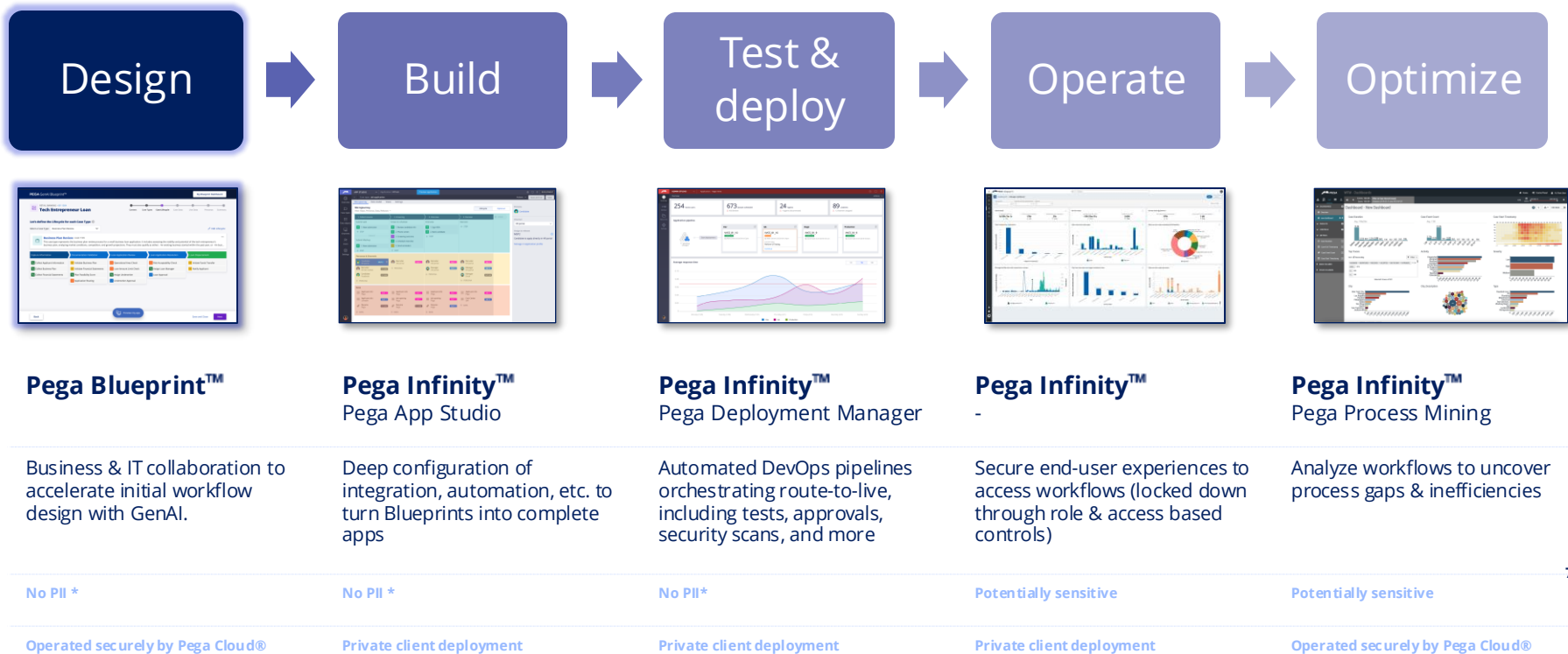
Jumpstart development.

Eliminate lengthy requirements gathering processes and set devs up for **rapid go-lives**:

- Import Blueprint to **generate app**, in seconds
- Auto-generate **user story backlog**
- Leverage AI across Pega App Studio to **quickly finalize & deploy new app**

Where does Blueprint fit in the SDLC?

Rapid design to jumpstart development



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

02

Blueprint architecture.



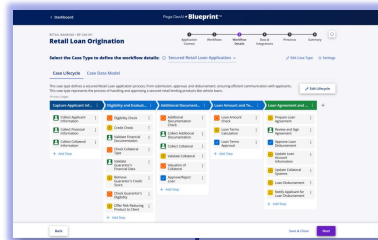
Pega Blueprint™ Architecture

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-East, UK, or European Union](#)).
- 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.com front-end web app



Pega.com auth service

Your SSO

Your employee
{user}@{your-org}.com



Fully isolated in region across:
US - UK - EU

PEGA Cloud® AWS

Blueprint application

Core processing of user requests & Blueprint functionality
Built on Pega Infinity™

Industry knowledge service

Retrieval augmented generation service which provides Blueprint with information on workflow & data model best practices based on user request.

Built on Pega Knowledge Buddy™. Contains Pega industry P.
Does not store any client or user data.

Pega Cloud AI Orchestration service

Orchestrates calls to LLM's

Built on AWS. Does not store any prompts, client data, or user data.



AWS Bedrock
Primary LLM provider
Claude, Haiku & Sonnet



Google Gemini
Flash



Azure OpenAI
GPT

Various LLM's leveraged based on use case / performance. All processing in region.
No AI trained on user or enterprise data.



Secure data storage

Enterprise private data-at-rest encryption (DARE)

All client data stored in volume & data bases encrypted with 256-bit encryption. By default, encryption keys rotate on a regular basis and are securely stored in a secure FIPS 140-2 compliant KMS.

Enterprise private encryption keys available upon request.



Private file storage




Connect to your Pega Cloud repo

All files related to Blueprint activity - for example uploaded documentation & videos are stored in an enterprise private S3 folder. By default, this is an S3 folder managed on behalf of the enterprise by Blueprint.
Pega Cloud clients can choose to store Blueprint-related files in their existing private S3 repository associated with their Pega Cloud instance upon request.

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




Enterprises located in the European Union

- Storage & compute: **AWS EU-Central (Frankfurt)**
- [AI Model Execution](#): In region

	Provider	Model / provider	LLM regions
	AWS Bedrock <small>Primary provider</small>	Anthropic	AWS Bedrock: European Union
	Google Gemini	Flash	Google Vertex: European Union
	Microsoft Azure	GPT	Microsoft Azure: European Union

Enterprises located in the United Kingdom

- Storage & compute: **AWS EU-WEST-2 (London)**
- [AI Model Execution](#): In region

	Provider	Model / provider	LLM regions
	AWS Bedrock <small>Primary provider</small>	Anthropic	AWS Bedrock: United Kingdom
	Google Gemini	Flash	Google Vertex: United Kingdom
	Microsoft Azure	GPT	Microsoft Azure: United Kingdom

Enterprises located Across the globe

- Storage & compute: **AWS US-East**
- [AI Model Execution](#): In region

	Provider	Model / provider	LLM regions
	AWS Bedrock <small>Primary provider</small>	Anthropic	AWS Bedrock: United States
	Google Gemini	Flash	Google Vertex: United States
	Microsoft Azure	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](#): In region

	Provider	Model / provider	LLM regions
	AWS Bedrock <small>Primary provider</small>	Anthropic	AWS Bedrock: Sydney
	Google Gemini	Flash	Google Vertex: Sweden
	Microsoft Azure	GPT	Microsoft Azure: Sweden

Enterprises located in the

Japan




- Storage & compute: **AWS: Japan - Osaka**
- [AI Model Execution](#): In region

	Provider	Model / provider	LLM regions
	AWS Bedrock <small>Primary provider</small>	Anthropic	AWS Bedrock: Japan - Osaka
	Google Gemini	Flash	Google Vertex: Sweden
	Microsoft Azure	GPT	Microsoft Azure: Sweden

Enterprises located

Singapore

- Storage & compute: **AWS: Singapore**
- [AI Model Execution](#): In region

	Provider	Model / provider	LLM regions
	AWS Bedrock <small>Primary provider</small>	Anthropic	AWS Bedrock: Singapore
	Google Gemini	Flash	Google Vertex: Sweden
	Microsoft Azure	GPT	Microsoft Azure: Sweden

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.

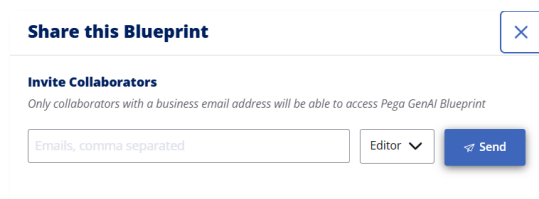
What we need from you: SAML 2.0 Configuration details or OAuth Configuration details

Login to following applications will use Federated authentication: Blueprint, Pega.com, community.pegacom, academy.pegacom, support.pegacom, docs.pegacom, partners.pegacom, saleshub.pegacom, partner-logo-generator.pegacom, 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*.



Share this Blueprint

Invite Collaborators
Only collaborators with a business email address will be able to access Pega GenAI Blueprint

Emails, comma separated

Editor ▼

Send

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.

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.

Pega Blueprint™ Data Visibility

Data Remains Confidential

The details of your Blueprints are stored in an encrypted database. Those details are visible only to authorized Pega administrative personnel. And the data you put into Blueprint isn't used to train any of the AI models we use. No data (prompts or responses) is shared with the LLM providers nor accessible to cloud providers. The information stays yours and yours alone.



What do users at Pega actually see?

Just the minimum needed to keep the system working and help us engage with you when you need help:

- The **system-generated identifier** of the blueprint. Your blueprint creates a Pega case, and this is the case ID.
- The **email address** of the person who created your blueprint
- The **short name** you've provided for your blueprint

Everything else?

Completely private. Your process descriptions, your workflows, your data models, and any documents you upload – including application docs, BPMN files, API definitions, or integration configurations – remain private to you as described above.

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](#)

The screenshot shows the Pega Cloud Trust Center website. At the top, there's a navigation bar with the Pega logo and links for Platform, Solutions, Customers, Learn, Services & Partners, Events, and About. Below this is a banner for the Pega Trust Center with the text: "Secure. Reliable. Compliant. Pega Cloud empowers the world's biggest brands to meet - and exceed - the challenges of today and tomorrow. Learn how." A link "Learn more about Pega's security features:" is provided. The main content area is divided into sections: Security, Authorization & access, Client-based access control, Network protection, Data encryption, and Secure system integration. Each section has a brief description and a link to "View security features". Below this is a section for "Supporting security documents" with a table of resources. The table has columns for Resources, Last updated (YYYY-MM-DD), and Assessment scope. The resources listed are: Pega Security Policies (2018-12-27), Pega Cloud AWS, GCP; Pega Security Statement (N/A), Pega Cloud AWS, GCP; Pega Security Test Summaries (2024-09-17), Pega Cloud AWS, GCP; Pega Security Business Continuity Plan Summary (2024-05-03), Pega Cloud AWS, GCP; Pega Security Disaster Recovery Test Results (2018-12-09), Pega Cloud AWS, GCP. Below the table is a section for "Privacy" with a link to "Read Pega's privacy notice". At the bottom, there's a section for "Compliance certifications, attestations, and accessibility" with a link to "Pega Cloud certifications". This section includes a table of certifications: APRA, CS, CSA STAR, Cyber Essentials, Cyber Essentials Plus, CyberGRX, Cybervalds, and NIS.


Resources	Last updated (YYYY-MM-DD)	Assessment scope
Pega Security Policies	2018-12-27	Pega Cloud AWS, GCP
Pega Security Statement	N/A	Pega Cloud AWS, GCP
Pega Security Test Summaries	2024-09-17	Pega Cloud AWS, GCP
Pega Security Business Continuity Plan Summary	2024-05-03	Pega Cloud AWS, GCP
Pega Security Disaster Recovery Test Results	2018-12-09	Pega Cloud AWS, GCP

Certification	Link
APRA	View details
CS	View details
CSA STAR	View details
Cyber Essentials	View details
Cyber Essentials Plus	View details
CyberGRX	View details
Cybervalds	View details
NIS	View 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 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

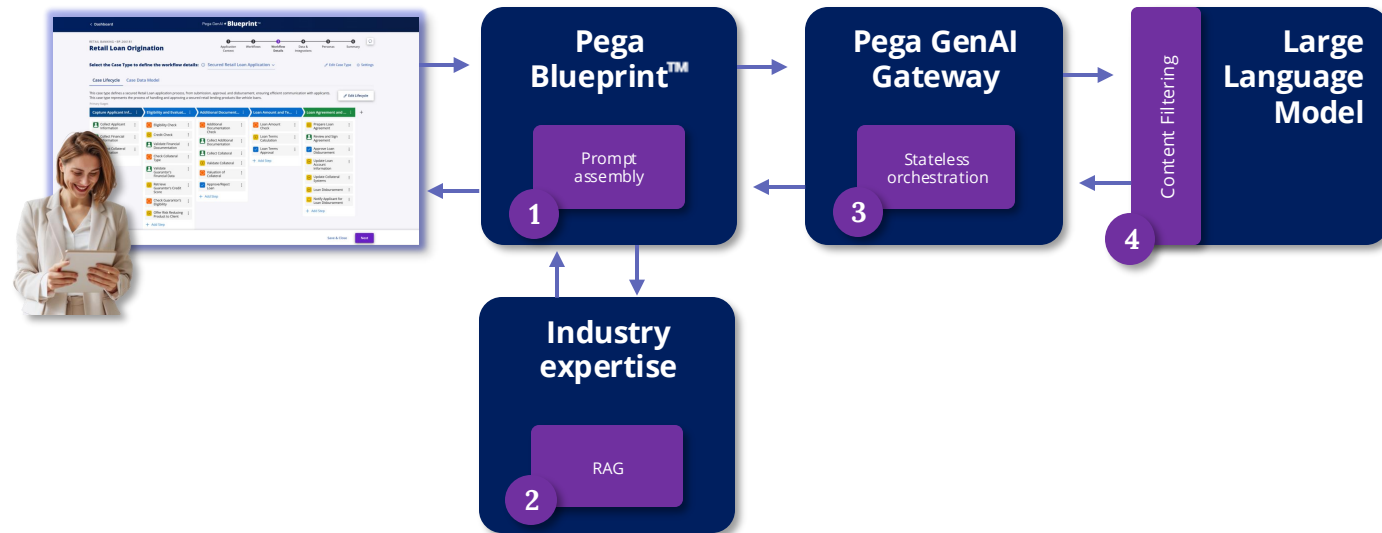
**Always up-to-date on [pega.com](https://www.pega.com)

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 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.

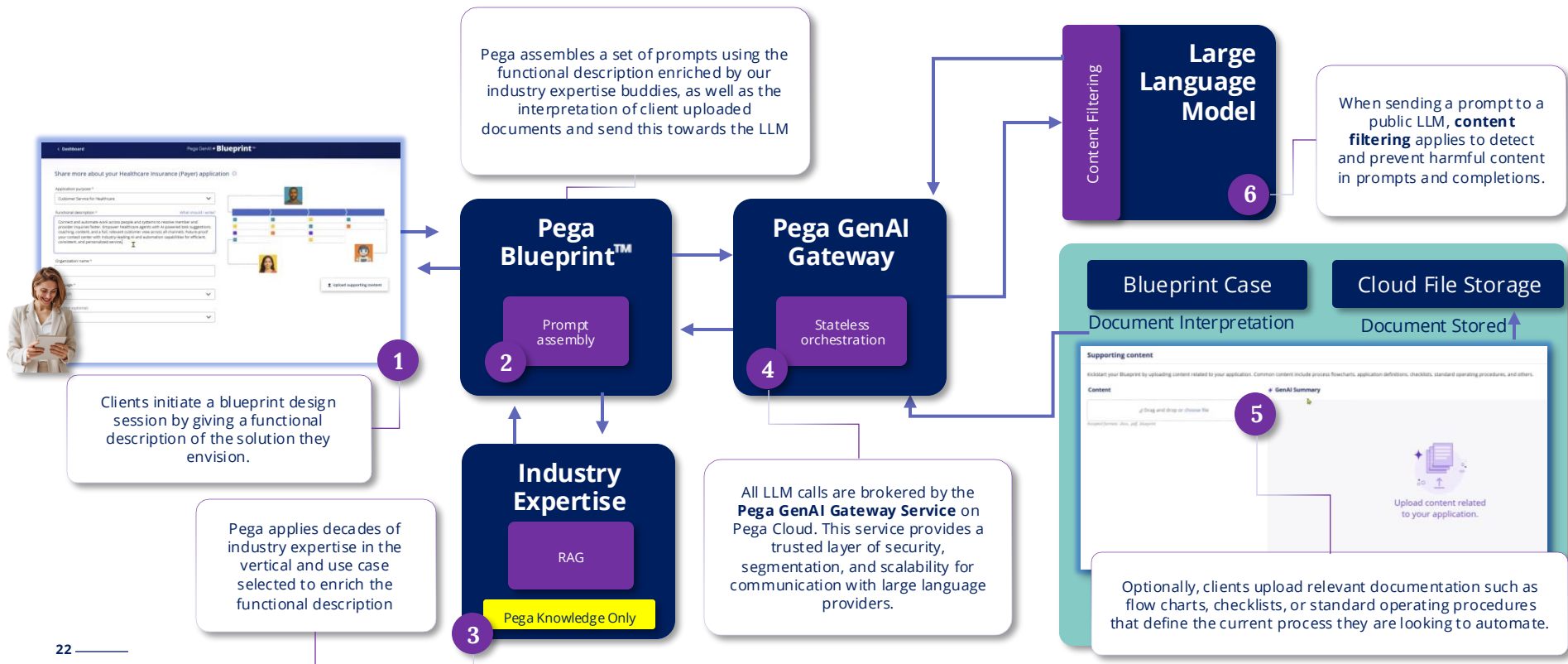
AI Data Flow

Pega Blueprint™

Content filtering approach

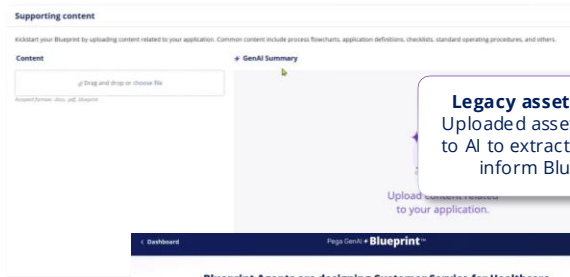
Pega relies on the most proven Large Language Model Providers in its delivery of Pega capabilities that rely on Generative AI. Within each model, are robust content filtering capabilities that will mitigate the possibilities of harmful, unethical, or toxic responses from occurring. While the capabilities 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.



AI Data Flow

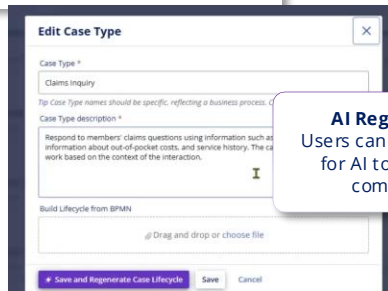
Pega Blueprint™



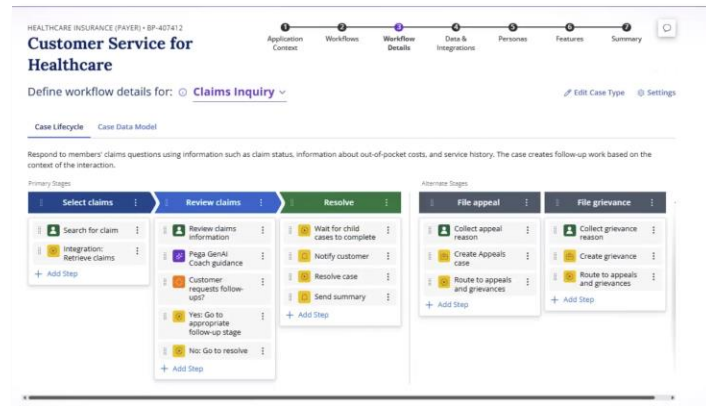
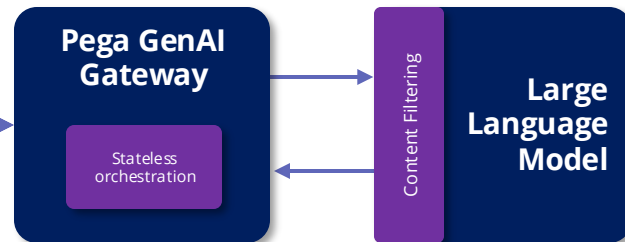
Legacy asset analysis
Uploaded assets are sent to AI to extract insights & inform Blueprint



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



AI Regeneration
Users can optionally ask for AI to regenerate components



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. Microsoft AI Red Team Methodology
2. OpenAI Safety Best Practices
3. Microsoft required mitigations
4. OWASP Top 10 for LLM Applications
5. 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.pegas.com>