



La trasformazione di cui ti puoi *fidare*.

Come Pega Blueprint gestisce in modo
sicuro dati, privacy e IA.

— Pega Blueprint™ - Sicurezza e privacy



< Dashboard Pega GenAI • **Blueprint™**

RETAIL BANKING • DP-206181

Retail Loan Origination

Application Context Workflows Worklist Details

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 ...
- Collect Applicant Information - Collect Financial Information - Collect Collateral Information + Add Step	- Eligibility Check - Credit Check - Validate Financial Documentation - Check Collateral Type - Validate Guarantor's Financial Data - Retrieve Guarantor's Credit Score - Check Guarantor's Eligibility - Offer Risk Reducing Product to Client + Add Step	- Additional Documentation Check - Collect Additional Documentation - Collect Collateral - Validate Collateral - Valuation of Collateral - Approve/Reject Loan + Add Step	- Loan Amount Check - Loan Terms Calculation - Loan Terms Approval + Add Step	- Prepare Loan Agreement - Review and Sign Agreement - Approve Loan Disbursement - Update Loan Account Information - Update Collateral Systems - Loan Disbursement - Notify Applicant for Loan Disbursement + Add Step

Save & Close Next

Pega Blueprint™

Sicurezza e privacy

- Riepilogo

Abbiamo progettato Pega GenAI Blueprint™ mettendo al primo posto la privacy e la sicurezza. Siamo consapevoli che i processi aziendali non sono solo diagrammi e flussi di lavoro, ma rappresentano il vantaggio competitivo del business.



Accesso gestito dall'azienda

L'accesso a Blueprint può essere connesso all'accesso Single Sign-On aziendale.

- Blueprint gestisce l'accesso ai dati tramite il controllo degli accessi basato sui ruoli per garantire che i blueprint creati rimangano privati per l'autore a meno che non vengano condivisi intenzionalmente.
- Quando un utente lascia l'organizzazione, perde l'accesso ai blueprint non appena il suo stato o i suoi ruoli vengono aggiornati nel provider SSO dell'organizzazione.

Nessuna IA viene addestrata con i tuoi blueprint

Prompt, dati e progetti non vengono mai utilizzati a scopo di addestramento dei modelli IA.

- Blueprint utilizza diversi LLM sottostanti, tra cui modelli Anthropic su AWS, Google Gemini e OpenAI su MS Azure.
- Tutti gli LLM sono soggetti a una governance continua e a test e utilizzano le best practice dei fornitori per il filtraggio dei contenuti.

Riservatezza dei dati

I dettagli dei blueprint vengono archiviati in un database su cloud crittografato.

- Distribuzione nel cloud nell'area geografica più adatta all'azienda: Stati Uniti, Regno Unito, APAC o UE.
- Nessun dato viene condiviso tra clienti o partner Pega.
- I blueprint sono privati per l'autore a meno che non vengano condivisi intenzionalmente.
- Solo i dati dei report a livello di attività vengono utilizzati in Pega da personale autorizzato (indirizzo e-mail, ora creazione, autore)

Sicurezza del cloud di livello enterprise

I dati del blueprint beneficiano della stessa protezione affidabile dell'ambiente di produzione Pega Cloud, che include:

- Crittografia AES a 256 bit per i dati inattivi e protezione HTTPS/TLS per i dati in transito.
- Monitoraggio continuo con sistemi di protezione antivirus e antintrusione basati su host.
- Centri operativi all'avanguardia che garantiscono elevati standard di sicurezza fisica e ambientale.
- Protezioni integrate contro gli attacchi DDoS e il blocco automatico degli indirizzi IP dannosi noti.



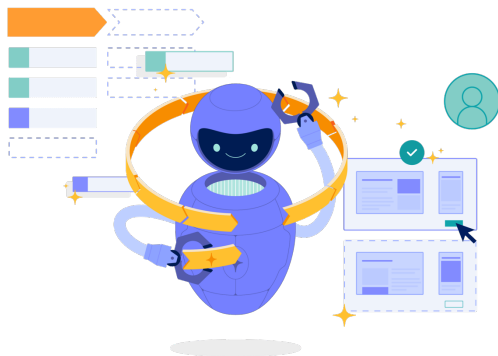
01

Che cos'è Pega Blueprint?



Volano di trasformazione

Pega Blueprint consente lo sviluppo di flussi di lavoro aziendali basati sull'IA. Pensato per unire persone e IA, accelerare l'automazione e la trasformazione.



Pega GenAI + Blueprint™

Dashboard

RETAIL BANKING • BP-266181

Retail Loan Origination

Select the Case Type to define the workflow details: [Secured Retail Loan Application](#) [Edit Case Type](#) [Settings](#)

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. [Edit Lifecycle](#)

Primary Stages

Capture Applicant Inf...	Eligibility and Evaluat...	Additional Document...	Loan Amount and Te...	Loan Agreement and ...
- Collect Applicant Information - Collect Financial Information - Collect Collateral Information + Add Step	- Eligibility Check - Credit Check - Validate Financial Documentation - Check Collateral Type - Validate Guarantor's Financial Data - Retrieve Guarantor's Credit Score - Check Guarantor's Eligibility - Offer Risk Reducing Product to Client + Add Step	- Additional Documentation Check - Collect Additional Documentation - Collect Collateral - Validate Collateral - Valuation of Collateral - Approve/Reject Loan + Add Step	- Loan Amount Check - Loan Terms Calculation - Loan Terms Approval + Add Step	- Prepare Loan Agreement - Review and Sign Agreement - Approve Loan Disbursement - Update Loan Account Information - Update Collateral Systems - Loan Disbursement - Notify Applicant for Loan Disbursement + Add Step

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



Come si colloca Blueprint nell'SDLC?

Progettazione rapida per accelerare lo sviluppo



*Basato sui casi d'uso sul tempo di progettazione, si sconsiglia di gestire le PII in queste fasi

02

Architettura di Blueprint



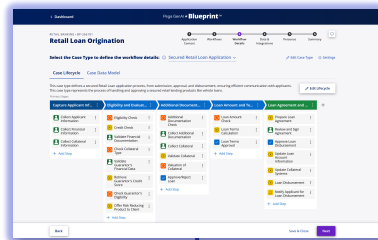
Pega Blueprint™ Architettura

Blueprint viene eseguito in modo sicuro in Pega Cloud® su AWS, gestito e utilizzato seguendo [standard cloud leader di settore](#).

Architettura di alto livello:

- L'autenticazione Blueprint si connette al protocollo SSO (Single Sign-On Protocol) aziendale.
- Pega offre servizi di residenza dei dati geograficamente segmentati specifici per la soluzione Pega Cloud. L'area geografica Blueprint si basa sulla sede della tua azienda ([negli Stati Uniti, nel Regno Unito, nell'Unione Europea, in Australia, a Singapore o in Giappone](#)).
- L'elaborazione dei blueprint viene eseguita su un'applicazione Pega Infinity sicura e affidabile, completamente supportata dalla potenza operativa dei Pega Cloud Services, che offre [affidabilità](#), [conformità](#), [sicurezza](#) e [disaster recovery](#) di livello enterprise.
- Blueprint utilizza gli LLM in base al caso d'uso e alle prestazioni. Principalmente modelli Claude in esecuzione su [AWS Bedrock](#).
- Nessuna IA viene addestrata con i dati di Blueprint.
- I dati del blueprint vengono [crittografati in transito](#) con TLS.
- I dati di Blueprint vengono [archiviati in modo sicuro e crittografati a riposo](#).

App web front-end Pega.com



App web front-end
autenticazione

Il tuo
SSO

Il tuo dipendente
{utente}@{organizzazione}.com



Completamente isolato nell'area geografica in:
USA — UE — AUS

PEGA Cloud® AWS



Applicazione Blueprint

Elaborazione di base delle richieste utente e funzionalità Blueprint

Basato su Pega Infinity™



Servizio di conoscenza del settore

Servizio di generazione aumentata di recupero che fornisce a Blueprint informazioni su best practice per flussi di lavoro e modelli di dati base alla richiesta dell'utente.

Basato su Pega Knowledge Buddy™. Contiene la proprietà intellettuale di settore di Pega. Non memorizza i dati dei clienti o degli utenti.



Servizio di orchestrazione dell'IA Pega Cloud

Orchestra le chiamate agli LLM

Basato su AWS. Non memorizza prompt, dati di clienti o dati utente.



AWS Bedrock
Fornitore principale di LLM
Claude Haiku & Sonnet



Google
Gemini
Flash



Azure
OpenAI
GPT

Vari LLM utilizzati in base al caso d'uso/alle prestazioni. Tutte le elaborazioni avvengono nell'area geografica di pertinenza. Nessuna IA addestrata con i dati utente o aziendali.



Storage sicuro dei dati

Crittografia dei dati privati aziendali a riposo (DARE)

Tutti i dati dei clienti archiviati in volumi, database con crittografia a 256 bit. Per impostazione predefinita, le chiavi di crittografia vengono ruotate regolarmente e archiviate in modo sicuro in un servizio di gestione protetto conforme allo standard FIPS 140-2.

Chiavi di crittografia private aziendali disponibili su richiesta.



Storage privato dei file

Connettiti al tuo repository Pega Cloud

Tutti i file relativi all'attività di Blueprint, ad esempio la documentazione e i video caricati, vengono archiviati in una cartella di archiviazione dei file Pega Cloud privata dell'azienda. Per impostazione predefinita, si tratta di una cartella gestita per conto dell'azienda da Blueprint. I file relativi al Blueprint dei clienti di Pega Cloud sono memorizzati per impostazione predefinita nel loro repository di archiviazione file Pega Cloud privato esistente, associato alla loro istanza di Pega Cloud.

Pega Blueprint™ – Residenza locale dei dati (UE, UK, USA)

In locale presso l'azienda in

Unione Europea

- Storage e calcolo: **AWS EU-Central (Francoforte)**
- [Esecuzione del modello IA](#)

In locale presso l'azienda in

Regno Unito

- Storage e calcolo: **AWS EU-Central (Francoforte)**
- [Esecuzione del modello IA](#)

In locale presso l'azienda in

Tutto il mondo

- Storage e calcolo: **AWS US-East**
- [Esecuzione del modello IA](#)

	Provider	Modello / fornitore	Aree LLM
	AWS Bedrock Fornitore principale	Anthropic	AWS Bedrock: Unione Europea
	Google Cloud	Gemini	Google Vertex: Unione Europea
	Microsoft Azure	OpenAI - GPT	Microsoft Azure: Unione Europea

	Provider	Modello / fornitore	Aree LLM
	AWS Bedrock Fornitore principale	Anthropic	AWS Bedrock: Unione Europea
	Google Cloud	Gemini	Google Vertex: Unione Europea
	Microsoft Azure	OpenAI - GPT	Microsoft: Unione Europea

	Provider	Modello / fornitore	Aree LLM
	AWS Bedrock Fornitore principale	Anthropic	AWS Bedrock: Stati Uniti
	Google Cloud	Gemini	Google Vertex: Stati Uniti
	Microsoft Azure	OpenAI - GPT	Microsoft Azure: Stati Uniti

Per partner Pega

Nella pagina della descrizione funzionale, indica il nome dell'azienda per cui stai creando il blueprint in modo che venga archiviato e gestito all'interno dell'area geografica da parte di tale azienda, automaticamente.

Determinazione dell'area geografica in cui viene archiviato il blueprint

Verifica l'ID del blueprint, che mostra un identificatore locale se archiviato e gestito in Unione Europea, Australia, Regno Unito, Giappone o Singapore.

Pega Blueprint™ – Residenza locale dei dati (APAC)

In locale presso l'azienda in

Australia

- Archiviazione e calcolo: **AWS: Australia - Sydney**
- [Esecuzione del modello IA](#)

Provider	Modello / fornitore	Aree LLM
 AWS Bedrock Fornitore principale	Anthropic	AWS Bedrock: Australia
 Google Cloud	Gemini	Google Vertex: Australia
 Microsoft Azure	OpenAI - GPT	Microsoft Azure: Australia

In locale presso l'azienda in

Giappone

- Archiviazione e calcolo: **AWS: Giappone - Osaka**
- [Esecuzione del modello IA](#)

Provider	Modello / fornitore	Aree LLM
 AWS Bedrock Fornitore principale	Anthropic	AWS Bedrock: Giappone/APA C
 Google Cloud	Gemini	Google Vertex: Japan
 Microsoft Azure	OpenAI - GPT	Microsoft Azure: Giappone / Unione Europea

In locale presso l'azienda in

Singapore

- Archiviazione e calcolo: **AWS: Singapore**
- [Esecuzione del modello IA](#)

Provider	Modello / fornitore	Aree LLM
 AWS Bedrock Fornitore principale	Anthropic	AWS Bedrock: APAC
 Google Cloud	Gemini	Google Vertex: Singapore
 Microsoft Azure	OpenAI - GPT	Microsoft Azure: Unione Europea

Per partner Pega

Nella pagina della descrizione funzionale, indica il nome dell'azienda per cui stai creando il blueprint in modo che venga archiviato e gestito all'interno dell'area geografica da parte di tale azienda, automaticamente.

Determinazione dell'area geografica in cui viene archiviato il blueprint

Verifica l'ID del blueprint, che mostra un identificatore locale se archiviato e gestito in Unione Europea, Australia, Regno Unito, Giappone o Singapore.

03

Accesso e autenticazione



Pega Blueprint™

Accesso e autenticazione

Configura l'accesso a Blueprint con il Single Sign-On (SSO).

Consentire agli utenti di autenticarsi tramite l'IDP dell'organizzazione garantisce che solo gli utenti autorizzati accedano a TUTTI i siti e le applicazioni Pega, come Blueprint, My Support Portal, ecc.

Quando l'autenticazione federata è abilitata, al momento dell'accesso agli utenti non verrà richiesto di fornire una password e verranno reindirizzati per l'autenticazione presso il proprio provider di servizi di identità.

I responsabili IT dell'organizzazione cliente possono collaborare con il nostro team account integrato per abilitare l'autenticazione federata.

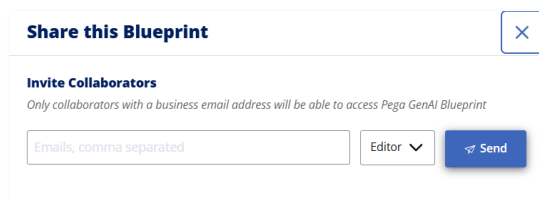
Cosa occorre: **dettagli della configurazione SAML 2.0** o **dettagli della configurazione OAuth**

L'accesso alle seguenti applicazioni utilizza l'autenticazione federata: 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, portale di supporto, My Pega Cloud, My Pega, PDC, Deployment Manager, Pega Trials

I blueprint sono visibili solo all'autore, a meno che non vengano condivisi intenzionalmente.

Per impostazione predefinita, i blueprint non sono visibili a nessuno al di fuori dell'utente che li ha creati (*proprietario* del blueprint).**

I proprietari del blueprint hanno la possibilità di condividerlo con altri stakeholder (ad es. membri del team, partner, ecc.). Possono invitare gli utenti via e-mail come *editor* o *visualizzatori*.



Quando un utente lascia l'organizzazione, i suoi blueprint restano nell'organizzazione.

Se un'azienda ha federato il proprio SSO con le proprietà digitali di Pega (ad es. Blueprint), solo gli utenti con accesso attivo al proprio SSO possono accedere a Blueprint.

Se un utente modifica il dominio registrato con il proprio profilo pega.com, ad esempio cambia organizzazione, i blueprint creati all'interno del vecchio dominio non saranno più visibili.

L'accesso a tali blueprint può essere ripristinato per altri utenti all'interno dell'organizzazione su richiesta.

**Visibile solo al personale amministrativo autorizzato per le operazioni cloud di Pega.

04

Privacy dei dati



Pega Blueprint™

Gestione dati

Quali dati vengono acquisiti e come vengono gestiti?

N.	Punto dati	Formato	Elaborati da LLM?	Utilizzati per addestramento IA?	Archiviati in...	Visibili a...
1	Dati dell'autore	Metadati (nome, e-mail, organizzazione)	No	No	Archiviazione dati Pega Cloud Completamente crittografati*	Pega
2	Descrizione app	Metadati (settore, nome dell'app)	Sì. A scopo di definizione del modello di blueprint iniziale	No	Archiviazione dati Pega Cloud Completamente crittografati*	Pega
3	Descrizione dell'applicazione basata su testo	Testo crittografato	Sì. A scopo di definizione del modello di blueprint iniziale	No	Archiviazione dati Pega Cloud Completamente crittografati*	Solo autore del blueprint e utenti invitati**
4	Documentazione legacy	.PDF, .DOC, .DOCX	Sì. A scopo di definizione del modello di blueprint iniziale	No	Archiviazione file Pega Cloud Crittografati a riposo*	Solo autore del blueprint e utenti invitati**
5	Video e immagini legacy	.MOV, .MP4, .JPG, .PNG	Sì. A scopo di definizione del modello di blueprint iniziale	No	Archiviazione file Pega Cloud Crittografati a riposo*	Solo autore del blueprint e utenti invitati**
6	Diagrammi di processo	.BPMN	Sì. A scopo di definizione del modello di blueprint iniziale	No	Archiviazione file Pega Cloud Crittografati a riposo*	Solo autore del blueprint e utenti invitati**
7	Integrazione e documentazione dati	.YAML, .SQL, .DDL, .CRD	Sì. A scopo di definizione del modello di blueprint iniziale	No	Archiviazione file Pega Cloud Crittografati a riposo*	Solo autore del blueprint e utenti invitati**
8	Modifiche al blueprint e progetti finali	Metadati crittografati (esportati come file .Blueprint crittografato)	No	No	Archiviazione dati Pega Cloud Completamente crittografati*	Solo autore del blueprint e utenti invitati**

*I dati del blueprint possono essere eliminati definitivamente su richiesta tramite l'assistenza Pega.

**Visibile solo al personale amministrativo autorizzato per le operazioni cloud di Pega.

05

Sicurezza del cloud





Una trasformazione su cui puoi contare

- Monitoraggio, gestione e supporto delle operazioni 24 ore su 24, 7 giorni su 7
- Operazioni dell'architettura sicure fin dalla progettazione con rigorosi controlli degli accessi e salvaguardie operative, riducendo al minimo il contatto umano attraverso l'automazione
- Conformità, tempi di attività, disaster recovery e modellazione delle minacce di livello aziendale enterprise

Operazioni

Monitoraggio 24 ore su 24, 7 giorni su 7, supporto ambientale e risposta proattiva

[Dettagli](#)

Accesso

Ambiente governato da controlli operativi automatizzati e protocolli di accesso rigorosi

Dettagli

Conformità

Rigoroso rispetto di oltre 20 standard di settore

[Dettagli](#)

Disaster recovery

Backup completo di dati e servizi, failover e ripristino

Dettagli

Modellazione delle minacce

Segui la metodologia del red team basata sulla top 10 OWASP

Dettagli

Disponibilità

L'architettura sfrutta l'alta disponibilità e il disaster recovery integrati per supportare tempi di attività quasi continui.

[Dettagli](#)



[Pega Sites](#)
[Pega Solutions](#)
[Customers](#)
[Learn](#)
[Services & Partners](#)
[Events](#)
[About](#)


[Try Pega](#)

[!\[\]\(05101934568a7fa69c25399d8b3fab00_img.jpg\)
 Apache Log4j vulnerability update: Learn what steps Pega is taking to address this](#)

Pega Trust Center

Secure. Reliable. Compliant. Pega Cloud empowers the world's biggest brands to meet – and exceed – the challenges of today and tomorrow. Learn how.

Learn more about Pega's security features:

[Security](#)
[Privacy](#)
[Compliance](#)
[VPATs](#)
[Service reliability](#)

Security

Our security policies provide a framework for safeguarding against unauthorized access and preventing/mitigating attacks that compromise performance and availability.

[View security bulletins](#)

Authorization & access

Manager user and system data access with role-based controls to Pega Cloud Environments. Simplify native identity access management and integration with leading single sign-on technologies, including SAML, Okta, and Active Directory.

Client-based access control

Client-based access control rules define where and how customer data is stored and accessed. We associate personal data with actual people, not abstract entities such as businesses.

Network protection

Our network architecture is designed to meet a range of security control requirements. Gain secure operation of your Pega Cloud Environment(s) isolated from fellow Pega clients and internal services thanks to our network rulesets and access controls.

Data encryption

Encryption is critical to the protection of data whether it is in transit or at rest. Pega Cloud employs encryption across all Pega Cloud Environment(s) that meet or exceed client and regulatory requirements. When data is at rest, AES 256-bit encryption is the standard. For data in transit, Pega Cloud offers TLS 1.2 and TLS 1.3.

Secure system integration

We offer multiple secure and private ways for Pega Cloud Environment(s) to integrate with systems in enterprise environments.

Supporting security documents

Pega maintains a set of documents and white papers that allow our clients to better understand our overall security posture from software development through service delivery.

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

Privacy

Use our security to enable you to implement your own privacy and compliance strategies. We continually evolve our platform to provide the features and security measures that you may use to support your security and privacy strategy.

[Read Pega's privacy notice](#)

Compliance certifications, attestations, and accessibility

When evaluating the services listed under each compliance standard it should be noted that Pega relies on a common set of controls for the purposes of adherence. These common controls exist across the Pega Platform, the underlying infrastructure, and the operations, administration and management provided by Pega in Pega Cloud. Pega applications developed within the Pega Platform inherit these controls which are attested to in the current scope.

Pega Cloud certifications

APRA	✓
CS	✓
CSA STAR	✓
Cyber Essentials	✓
Cyber Essentials Plus	✓
CyberGRX	✓
Cyberavids	✓
ENIS	✓

06

Governance dell'IA





Pega Blueprint™ sfrutta un mix di modelli di frontiera per favorire una rapida trasformazione

I modelli sono tutti gestiti in modo sicuro e incorporati nel prodotto per bilanciare efficacia e prestazioni.

Informazioni aggiornate al 3° trimestre 2025

Pega valuta costantemente gli LLM al fine di utilizzare il modello adatto a ogni lavoro. Ecco alcuni modelli attualmente utilizzati:

Hyperscaler	Fornitore di LLM	Area geografica di Blueprint	Area geografica di LLM
 AWS Fornitore principale	Anthropic	AMS (USA)	AWS Bedrock: Stati Uniti
		UE	AWS Bedrock: Unione Europea
		Regno Unito	AWS Bedrock: Regno Unito
 Google Cloud	Google Gemini	AMS (USA)	Google Vertex: Stati Uniti
		UE	Google Vertex: Unione Europea
		Regno Unito	Google Vertex: Regno Unito
 Microsoft Azure	OpenAI - GPT	AMS (USA)	Microsoft Azure: Stati Uniti
		UE	Microsoft Azure: Unione Europea
		Regno Unito	Microsoft Azure: Regno Unito

Tutti gli accordi con gli hyperscaler includono l'impegno che nessun prompt o dato inviato da Pega o dai clienti sia accessibile né dall'hyperscaler né dal fornitore di LLM.

*Dati aggiornati a giugno 2025

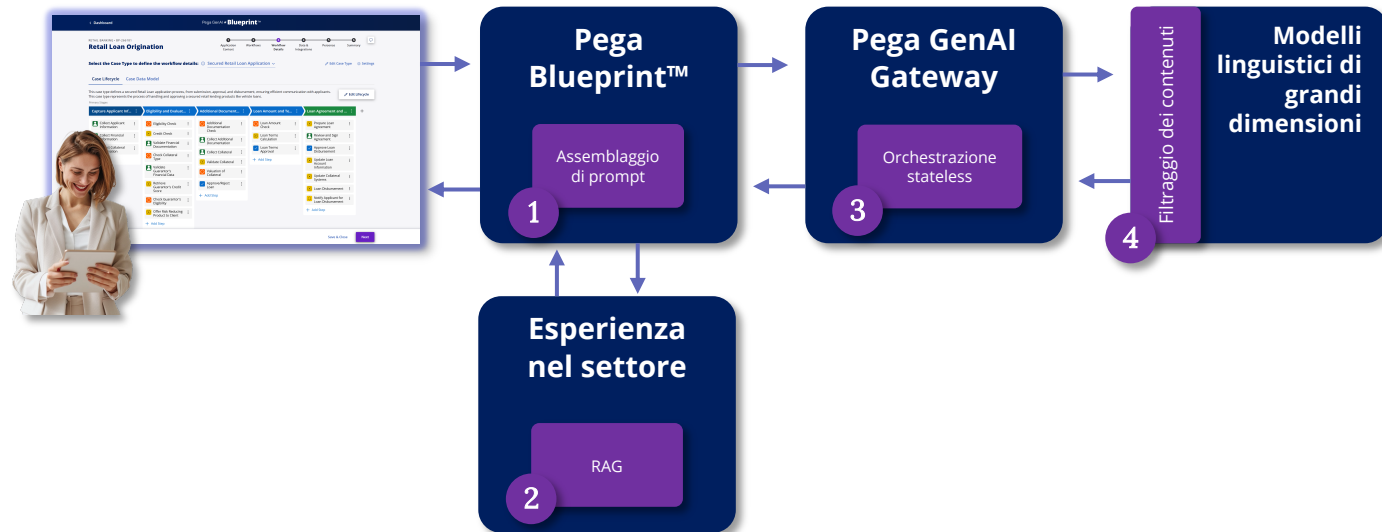
**Sempre aggiornati su pega.com

Flusso di dati IA

Pega Blueprint™

Gestione sicura dell'IA:

1. Pega Blueprint **crea prompt** che descrivono l'applicazione in base alle informazioni inserite dall'utente.
2. Pega Blueprint utilizza la **knowledge base di settore** di Pega eseguita su Pega Knowledge Buddy per sintetizzare le best practice sui casi d'uso di Blueprint e arricchire i prompt LLM e la creazione del blueprint.
3. Tutte le chiamate LLM sono mediate dal **Servizio Pega GenAI Gateway** su Pega Cloud. Il servizio offre un livello affidabile di sicurezza, segmentazione e scalabilità per la comunicazione con i fornitori di modelli linguistici di grandi dimensioni.
4. A un prompt crittografato inviato a un LLM protetto viene applicato il **filtraggio dei contenuti** per rilevare e prevenire contenuti dannosi nei prompt e nelle risposte.



Approccio al filtraggio dei contenuti

Pega si affida ai più collaudati fornitori di modelli linguistici di grandi dimensioni per le funzionalità Pega che si basano sull'IA generativa. Ogni modello integra solide funzionalità di filtraggio dei contenuti che mitigano il rischio di generare risposte dannose, non etiche o tossiche. Pur essendo efficaci, rappresentano esclusivamente misure di mitigazione e non escludono la possibilità di errore. Inoltre, ogni fornitore di modelli adotta un approccio diverso per ottenere un'IA responsabile ed etica.

Ciò significa che i modelli di classificazione, le soglie e le categorie di rilevamento possono differire. Quando vengono utilizzati modelli diversi, vengono applicati diversi tipi di classificazione e filtraggio dei contenuti. I clienti che utilizzano Pega GenAI Connect devono essere consapevoli di queste possibili differenze ed eseguire test per convalidarle.

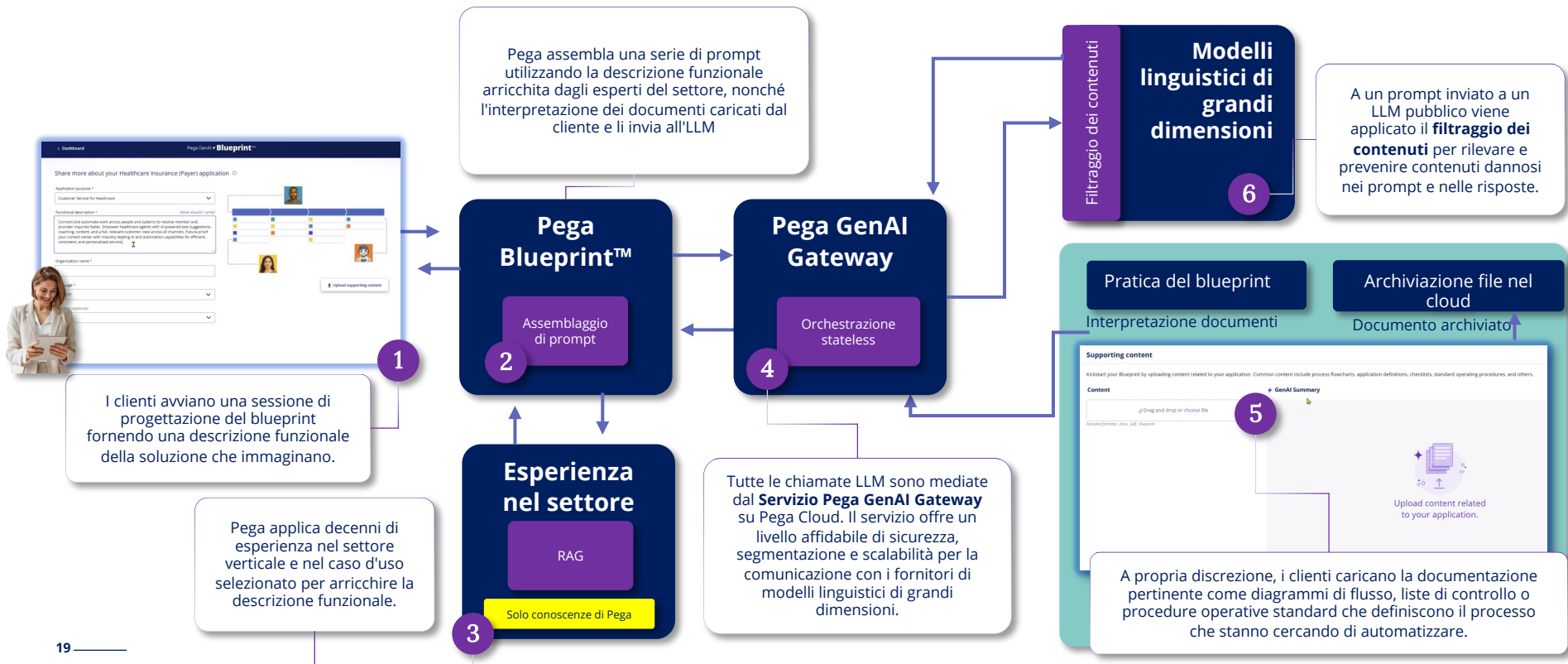
Flusso di dati IA

Pega Blueprint™

Approccio al filtraggio dei contenuti

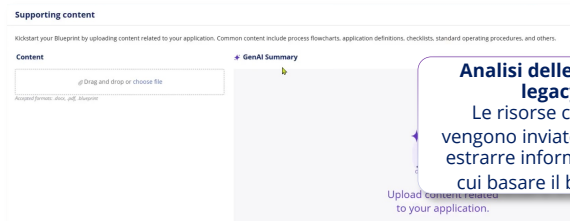
Pega si affida ai più collaudati fornitori di modelli linguistici di grandi dimensioni per le funzionalità Pega che si basano sull'IA generativa. Ogni modello integra solide funzionalità di filtraggio dei contenuti che mitigano il rischio di generare risposte dannose, non etiche o tossiche. Pur essendo efficaci, rappresentano esclusivamente misure di mitigazione e non escludono la possibilità di errore. Inoltre, ogni fornitore di modelli adotta un approccio diverso per ottenere un'IA responsabile ed etica.

Ciò significa che i modelli di classificazione, le soglie e le categorie di rilevamento possono differire. Quando vengono utilizzati modelli diversi, vengono applicati diversi tipi di classificazione e filtraggio dei contenuti. I clienti che utilizzano Pega GenAI Connect devono essere consapevoli di queste possibili differenze ed eseguire test per convalidarle.



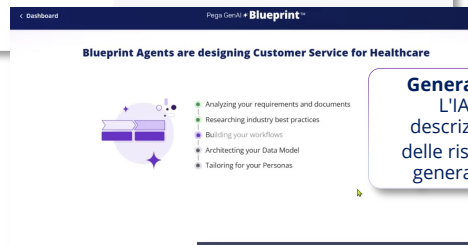
Flusso di dati IA

Pega Blueprint™



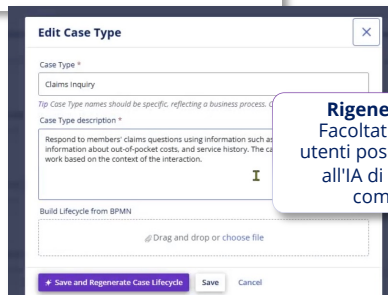
Analisi delle risorse legacy

Le risorse caricate vengono inviate all'IA per estrarre informazioni su cui basare il blueprint



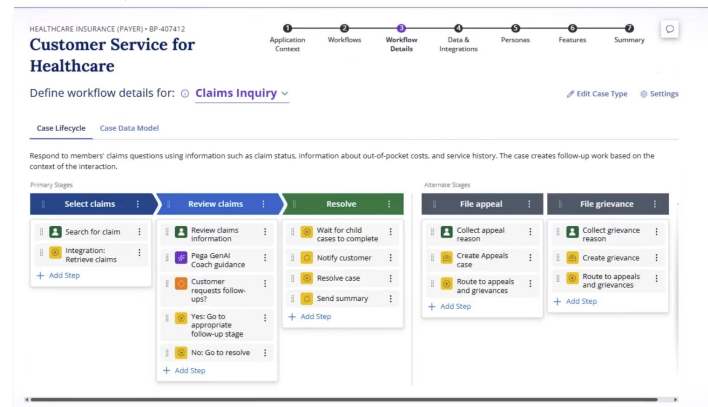
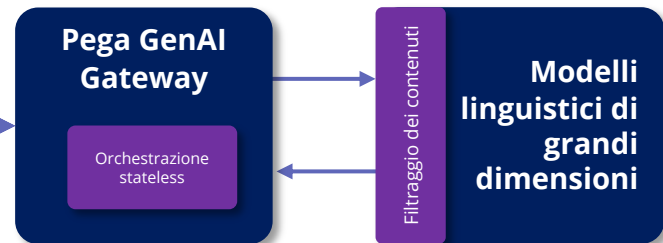
Generazione iniziale

L'IA analizza la descrizione e l'analisi delle risorse legacy per generare il blueprint



Rigenerazione IA

Facoltativamente gli utenti possono chiedere all'IA di rigenerare i componenti



Governance dell'IA in Pega

Supervisione end-to-end

Il comitato di Governance dell'IA di Pega è gestito dal team di sicurezza del cloud e supervisiona l'utilizzo dell'intelligenza artificiale nei prodotti Pega.

Riunisce esperti e proprietari di prodotti, sicurezza del cloud, operazioni su cloud, IT, legale e go-to-market per garantire che tutto l'utilizzo dell'intelligenza artificiale in Pega sia sicuro, responsabile e protetto.

Partnership strategiche

Al fine di soddisfare le esigenze specifiche dei suoi clienti aziendali, Pega ha stretto relazioni strategiche e accordi generali con AWS, Google Cloud e Microsoft per promuovere iniziative di intelligenza artificiale condivisa.

Pega e i suoi fornitori cloud di servizi LLM si incontrano regolarmente per esaminare le opzioni dei modelli, le prestazioni, la sicurezza e i problemi.

La sicurezza prima di tutto

Il comitato di governance dell'IA di Pega organizza ed esegue valutazioni continue della sicurezza di tutte le funzionalità basate sull'intelligenza artificiale, incluso Pega Blueprint.

Le valutazioni di sicurezza eseguite includono:

1. ISO 42001
2. Metodologia del Red Team di Microsoft AI
3. Best practice per la sicurezza di OpenAI
4. Soluzioni di prevenzione richieste da Microsoft
5. OWASP Top 10 per applicazioni LLM
6. OWASP Cloud-Native Application Security Top 10





Pega è l'azienda più importante nel settore della trasformazione aziendale e aiuta le organizzazioni a implementare la filosofia Build for Change® tramite decisioning basato su IA e automazione dei flussi di lavoro. Molte delle aziende più influenti del mondo si affidano alla nostra piattaforma per risolvere le sfide più urgenti, dalla personalizzazione dell'engagement all'automazione del servizio, fino alla semplificazione delle operazioni. Dal 1983, abbiamo costruito la nostra architettura basandoci su criteri di scalabilità e flessibilità per aiutare le aziende a soddisfare le richieste dei clienti di oggi e a trasformarsi continuamente per affrontare il futuro al meglio. Per ulteriori informazioni su Pega (NASDAQ: PEGA), consulta <http://www.pega.com/it>

