



Cloud Subscription Documentation

22 February 2024

CONTENTS

Pega Cloud subscription documentation_____ 3

Deployment regions. 6

Service operations and support. 22

Service connectivity. 25

Service level agreement. 26

Incident response and management. 28

Change management. 29

Disaster recovery. 32

Data backup, data restoration, and data durability. 34

Security standards. 37

Client data responsibilities. 42

Layered distributed denial of service protection. 46

Planning for end of subscription term. 48



Pega Cloud subscription documentation

Documentation for Pega Cloud subscriptions.

Pega Cloud provides a fully-managed Cloud Service platform running Pega software in an as-a-service model. Pega Cloud contains several additional cloud services that enhance Pega Customer Service Customer Engagement, Pega Sales Automation, and Client Onboarding.

Pega Cloud is managed by Pega, with global and regional support models for 24 x 7 operations, security, and monitoring to help support our clients' enterprise applications. Clients can forgo the complexities of operating and managing a Pega ecosystem in favor of letting Pega manage it for them. Pega Cloud allows Pega clients to get started quickly (within days of contract signature) and to realize the value of Pega solutions more rapidly.

Additional Cloud Services

Additional services available for use with Pega Cloud include:

Pega Deployment Manager (v6)

Deployment Manager is the standard way to test and deploy Pega applications. It exposes all capabilities of the Pega Platform necessary to automate a client's DevOps workflows, including branch merging, application packaging, applying quality gates, and promoting an application to different environments.

Deployment Manager leverages market-leading case management technology to build and run continuous integration and continuous delivery (CI/CD) pipelines with a familiar, model-driven experience.

Pega Predictive Diagnostic Cloud

Pega Predictive Diagnostic Cloud (PDC) is an intelligent agent that predicts, prioritizes, and notifies administrators about the health of a client's Pega



applications. It leverages artificial intelligence (AI) to provide operations teams a prioritized list of action plans that provide performance and stability.

Pega Workforce Intelligence

Pega Workforce Intelligence(WFI) leverages Task Mining capabilities, enabling clients to identify inefficient processes impacting employees and customers. Clients deploy AI-powered discovery bots that work around the clock, collecting information that provides an ongoing view into tasks performed by their teams. Desktop information reveals application usage, processes performed, and more, helping managers to understand the obstacles and distractions that undermine productivity.

Pega Process Mining

Pega Process Mining helps clients visualize processes to identify issues - such as bottlenecks and reworks - while quickly understanding the next best area of improvement. Clients can leverage Process Mining to analyze their Pega Applications or other critical systems they would like to optimize..

Pega Digital Messaging

The Digital Messaging service enables Pega Customer Service Digital Customer Engagement Edition clients to connect their cloud or on-premises Customer Service application to Pega's supported digital channels. Clients can implement one or more digital channels to support their customer engagement programs, and can configure the channels to provide automated assistance and transfer to a live agent.

Pega Co-Browse

Pega Co-Browse provides a live collaboration tool that allows clients' customer service agents to be able to see what the clients' customer is seeing. In Pega Co-Browse, clients can mask sensitive customer data; agents have annotation tools to aid their customers in completing their tasks.

Legacy Web Chat (formerly Pega Chat)

Legacy Web Chat provides a chat channel for Customer Service Representatives (CSRs) to interact with clients' customers. Clients can implement several self-service options in chatbots, including service cases, proactive chat, and Pega



Knowledge articles. Clients' customers can receive automated assistance and transfer to a live agent for CSR assistance.

Pega Voice AI

Pega Voice AI helps clients' customers, employees and developers reduce complexity, engage more effectively, and drive positive outcomes. Voice AI uses natural language processing in tandem with Pega's intelligent automation capabilities to detect intent, surface relevant knowledge, and automate actionable work in real-time.

Pega GenAI

Pega GenAI allows clients to use a set of inputs (known as prompts) that leverage Artificial Intelligence (which is capable of generating text or other media) to render an outcome or output. Inputs are either created by Pega or authored by clients within Pega Infinity. Outcomes or outputs may include simplified application design and authoring, synthesis of text into insights using comprehensive text, visualizations, content creation suggestions, and intuitive usability improvements.

The Subscription Documentation also includes:

- The [Vulnerability Testing Policy for applications on Pega Cloud](#), which describes how Pega Cloud clients can conduct application security assessments, when such assessments are preauthorized and performed within the stated guidelines.
- The [Pega Cloud Acceptable Use Policy](#), which describes the permitted and prohibited activities for clients in their Pega Cloud environments.

Pega may occasionally make changes to this Subscription Documentation. However, Pega will not make changes that materially diminish clients' rights for currently supported Pega Cloud services.

For additional Pega Cloud information which is not part of the Pega Cloud Subscription documentation, including Getting Started and How-Tos, see [Pega Cloud](#).

- [Deployment regions for Pega Cloud](#)
- [Service operations and support for Pega Cloud](#)



- **Service connectivity for Pega Cloud**
- **Service level agreement for Pega Cloud**
- **Incident response and management for Pega Cloud**
- **Change management for Pega Cloud**
- **Disaster recovery for Pega Cloud**
- **Data backup, data-restoration, and data durability for Pega Cloud**
- **Security standards for Pega Cloud**
- **Client data responsibilities Pega Cloud**
- **Layered distributed denial of service protection in Pega Cloud**
- **Planning for end of Pega Cloud subscription term**

Deployment regions for Pega Cloud

Deployment Regions list the cloud service locations available to our clients, including their selected region as identified in their client contract.



Notice: This article is part of the Pega Cloud Subscription Documentation. Only the full article (not a summary) is the official contractual document.

Pega Cloud offers several additional cloud services that enhance Pega Intelligent Automation, 1:1 Customer Engagement, Pega Customer Service, Pega Sales Automation, and Client Onboarding. The regions associated with these capabilities are paired with Pega's Deployment Regions, based on proximity and data sovereignty. Based on the client's selected Deployment Region, additional services they subscribe to will be located in the appropriate paired region.



Pega Cloud Deployment Regions

Pega Cloud clients may select one of the following available Deployment Regions.

Americas	EMEA	APAC
AWS: Canada – Central	AWS: Germany - Frankfurt	AWS: Singapore
AWS: USA – Northern Virginia	AWS: Ireland - Dublin	AWS: Australia - Sydney
AWS: USA - Ohio	AWS: United Kingdom - London	AWS: Japan - Tokyo
AWS: USA – Northern California	AWS: France - Paris	AWS: India – Mumbai
AWS: USA – Oregon	AWS: Sweden – Stockholm	AWS: Hong Kong
AWS: Brazil – Sao Paolo	AWS: Italy – Milan	AWS: Indonesia - Jakarta
	AWS: Switzerland - Zurich	AWS: South Korea - Seoul
GCP: Canada-Montreal	GCP: United Kingdom- London	
GCP: USA-Northern Virginia	GCP: Germany - Frankfurt	
GCP: USA-Oregon	GCP: Belgium - St. Ghislain	
GCP: Brazil – Sao Paolo	GCP: Italy - Milan	
	GCP: Netherlands - Eemshaven	

"AWS-" denotes a region provided by Amazon Web Services. "GCP-" denotes a region provided by Google Cloud Platform.

Service Deployment Regions

The following cloud services are available in the regions listed below and are chosen based on the client-selected Deployment Region. For example, if a client chose the



EMEA region *AWS-Germany-Frankfurt* for their selected Deployment Region, and also subscribed to Pega Workforce Intelligence, their WFI service would be deployed in the EMEA region of *Ireland-Dublin*.

Pega GenAI

Pega GenAI does not currently follow the prescriptive paired service deployment region model. In all Pega GenAI deployments, a Pega client-selected deployment region will leverage a region(s) from the available global Microsoft Azure deployment regions known as Pega GenAI Service Deployment Regions. At deployment time, Pega endeavors where possible to use a Region from the available Pega GenAI Service Deployment Regions which is a comparable region to the client-selected deployment region. Pega will pair a client-selected deployment region within the US or EU with a comparable Pega GenAI deployment region(s) also in the US or EU.

Pega Deployment Manager

Pega Deployment Manager (v6) is currently available to be deployed in the following regions:

Pega Deployment Manager Service Deployment Region:	Pairs with the following client-selected Deployment Regions:
AWS: USA – Northern Virginia	AWS: Canada – Central AWS: Brazil – Sao Paolo AWS: USA • Northern Virginia • Ohio • Northern California • Oregon



Pega Deployment Manager Service Deployment Region:	Pairs with the following client-selected Deployment Regions:
AWS: United Kingdom - London	AWS: United Kingdom - London
AWS: Germany - Frankfurt	AWS: Germany - Frankfurt AWS: Ireland - Dublin AWS: France - Paris AWS: Sweden – Stockholm AWS: Italy – Milan AWS: Switzerland - Zurich
AWS: Australia - Sydney	AWS: Singapore AWS: Australia - Sydney AWS: Japan - Tokyo AWS: India – Mumbai AWS: Hong Kong AWS: Indonesia - Jakarta AWS: South Korea - Seoul
GCP: USA-Northern Virginia	GCP: USA-Northern Virginia GCP: USA - Oregon

Pega Deployment Manager Service Deployment Region:	Pairs with the following client-selected Deployment Regions:
	GCP: Brazil - Sao Paolo GCP: Canada - Montreal
GCP: Germany - Frankfurt	GCP: Germany - Frankfurt GCP: Belgium - St. Ghislain GCP: Italy - Milan GCP: Netherlands - Eemshaven
GCP: United Kingdom - London	GCP: United Kingdom - London

Pega Predictive Diagnostic Cloud

Pega Predictive Diagnostic Cloud is currently available to be deployed in the following regions:

Pega Predictive Diagnostic Cloud Service Deployment Region:	Pairs with the following client-selected Deployment Regions:
AWS: USA – Northern Virginia	AWS: Canada – Central AWS: Brazil – Sao Paolo AWS: USA • Northern Virginia • Ohio • Northern California

Pega Predictive Diagnostic Cloud Service Deployment Region:	Pairs with the following client-selected Deployment Regions:
	• Oregon AWS: Singapore AWS: Australia - Sydney AWS: Japan - Tokyo AWS: India – Mumbai AWS: Hong Kong AWS: Indonesia - Jakarta AWS: South Korea - Seoul
	GCP: Canada - Montreal GCP: Brazil – Sao Paolo GCP: USA • Northern Virginia • Oregon
AWS: Ireland – Dublin	AWS: United Kingdom - London AWS: Ireland - Dublin AWS: Germany - Frankfurt AWS: France - Paris AWS: Sweden – Stockholm

Pega Predictive Diagnostic Cloud Service Deployment Region:	Pairs with the following client-selected Deployment Regions:
	AWS: Italy – Milan AWS: Switzerland - Zurich
	GCP: United Kingdom – London GCP: Belgium - St. Ghislain GCP: Germany - Frankfurt GCP: Italy - Milan GCP: Netherlands - Eemshaven

Pega Workforce Intelligence

Pega Workforce Intelligence is currently available to be deployed in the following regions:

Pega Workforce Intelligence Service Deployment Region:	Pairs with the following client-selected Deployment Regions:
AWS: USA – Oregon	AWS: Canada – Central AWS: Brazil – Sao Paolo AWS: USA • Northern Virginia • Ohio • Northern California • Oregon



Pega Workforce Intelligence Service Deployment Region:	Pairs with the following client-selected Deployment Regions:
	GCP: Canada - Montreal GCP: Brazil – Sao Paolo GCP: USA • Northern Virginia • Oregon
AWS: Ireland – Dublin	AWS: United Kingdom - London AWS: Ireland - Dublin AWS: Germany - Frankfurt AWS: France - Paris AWS: Sweden – Stockholm AWS: Italy – Milan AWS: Switzerland - Zurich GCP: United Kingdom - London GCP: Germany - Frankfurt GCP: Belgium - St. Ghislain GCP: Italy - Milan GCP: Netherlands - Eemshaven

Pega Workforce Intelligence Service Deployment Region:	Pairs with the following client-selected Deployment Regions:
AWS: Australia - Sydney	AWS: Singapore AWS: Australia - Sydney AWS: Japan - Tokyo AWS: India – Mumbai AWS: Hong Kong AWS: Indonesia - Jakarta AWS: South Korea - Seoul

Pega Process Mining

Pega Process Mining is currently available to be deployed in the following regions:

Americas	EMEA	APAC
AWS: Canada – Central	AWS: Germany - Frankfurt	AWS: Singapore
AWS: USA – Northern Virginia	AWS: Ireland - Dublin	AWS: Australia - Sydney
AWS: USA - Ohio	AWS: United Kingdom - London	AWS: Japan - Tokyo
AWS: USA – Northern California	AWS: France - Paris	AWS: India – Mumbai
AWS: USA – Oregon	AWS: Sweden – Stockholm	AWS: Hong Kong
AWS: Brazil – Sao Paolo	AWS: Italy – Milan	AWS: Indonesia - Jakarta
	AWS: Switzerland - Zurich	AWS: South Korea - Seoul

Pega Digital Messaging

Pega Digital Messaging is currently available to be deployed in the following regions:

Pega Digital Messaging Service Deployment Region:	Pairs with the following client-selected Deployment Regions:
AWS: USA – Northern Virginia	AWS: Brazil – Sao Paolo
	AWS: USA - Northern Virginia - Ohio - Northern California - Oregon
	AWS: Singapore
	AWS: Australia - Sydney
	AWS: Japan - Tokyo
	AWS: India – Mumbai
	AWS: Hong Kong
	AWS: Indonesia - Jakarta
	AWS: South Korea - Seoul
	GCP: Brazil – Sao Paolo
	GCP: USA - Northern Virginia - Oregon



Pega Digital Messaging Service Deployment Region:	Pairs with the following client-selected Deployment Regions:
AWS: Canada – Central	AWS: Canada – Central
	GCP: Canada – Montreal
AWS: Ireland – Dublin	AWS: United Kingdom - London
	AWS: Ireland - Dublin
	AWS: Germany - Frankfurt
	AWS: France - Paris
	AWS: Sweden – Stockholm
	AWS: Italy – Milan
	AWS: Switzerland - Zurich
	GCP: United Kingdom – London
	GCP: Belgium - St. Ghislain
	GCP: Germany - Frankfurt
	GCP: Italy - Milan
	GCP: Netherlands - Eemshaven

Pega Co-browse

Pega Co-browse is currently available to be deployed in the following regions:



Pega Co-browse Service Deployment Region:	Pairs with the following client-selected Deployment Regions:
AWS: USA – Northern Virginia	AWS: Brazil – Sao Paolo AWS: USA - Northern Virginia - Ohio - Northern California - Oregon AWS: Singapore AWS: Australia - Sydney AWS: Japan - Tokyo AWS: India – Mumbai AWS: Hong Kong AWS: Indonesia - Jakarta AWS: South Korea - Seoul
AWS: Canada – Central	GCP: Brazil – Sao Paolo
	GCP: USA - Northern Virginia - Oregon
AWS: United Kingdom - London	AWS: Canada – Central
	GCP: Canada – Montreal
AWS: United Kingdom - London	AWS: United Kingdom - London



Pega Co-browse Service Deployment Region:	Pairs with the following client-selected Deployment Regions:
	GCP: United Kingdom – London
AWS: Ireland – Dublin	AWS: Ireland - Dublin AWS: Germany - Frankfurt AWS: France - Paris AWS: Sweden – Stockholm AWS: Italy – Milan AWS: Switzerland - Zurich
	GCP: Belgium - St. Ghislain GCP: Germany - Frankfurt GCP: Italy - Milan GCP: Netherlands - Eemshaven

Legacy Web Chat

Legacy Web Chat (formerly Pega Chat) will service the following Deployment Regions out of these provider regions:

Legacy Web Chat Service Deployment Region:	Pairs with the following client-selected Deployment Regions:
AWS: USA – Northern Virginia	AWS: Canada – Central AWS: Brazil – Sao Paolo



Legacy Web Chat Service Deployment Region:	Pairs with the following client-selected Deployment Regions:
	AWS: USA - Northern Virginia - Ohio - Northern California - Oregon
	GCP: Canada - Montreal GCP: Brazil – Sao Paolo GCP: USA - Northern Virginia - Oregon
AWS: Ireland – Dublin	AWS: United Kingdom - London AWS: Ireland - Dublin AWS: Germany - Frankfurt AWS: France - Paris AWS: Sweden – Stockholm AWS: Italy – Milan AWS: Switzerland - Zurich
	GCP: United Kingdom - London

Legacy Web Chat Service Deployment Region:	Pairs with the following client-selected Deployment Regions:
	GCP: Germany - Frankfurt GCP: Belgium - St. Ghislain GCP: Italy - Milan GCP: Netherlands - Eemshaven
AWS: Australia - Sydney	AWS: Singapore AWS: Australia - Sydney AWS: Japan - Tokyo AWS: India – Mumbai AWS: Hong Kong AWS: Indonesia - Jakarta AWS: South Korea - Seoul

Voice AI

Pega Voice AI is currently available to be deployed in the following regions:

Pega Voice AI Service Deployment Region:	Pairs with the following client-selected Deployment Regions:
AWS: USA – Northern Virginia	AWS: Canada – Central AWS: Brazil – Sao Paolo



Pega Voice AI Service Deployment Region:	Pairs with the following client-selected Deployment Regions:
	AWS: USA - Northern Virginia - Ohio - Northern California - Oregon AWS: United Kingdom - London AWS: Ireland - Dublin AWS: Germany - Frankfurt AWS: France - Paris AWS: Sweden – Stockholm AWS: Italy – Milan AWS: Switzerland - Zurich AWS: Singapore AWS: Australia - Sydney AWS: Japan - Tokyo AWS: India – Mumbai AWS: Hong Kong AWS: Indonesia - Jakarta AWS: South Korea - Seoul

Pega Voice AI Service Deployment Region:	Pairs with the following client-selected Deployment Regions:
	GCP: Canada - Montreal GCP: Brazil – Sao Paolo GCP: USA • Northern Virginia • Oregon GCP: United Kingdom – London GCP: Belgium - St. Ghislain GCP: Germany - Frankfurt GCP: Italy - Milan GCP: Netherlands - Eemshaven

Data Residency

Pega offers geographically segmented data residency services specific to its Pega Cloud offering. When the client selects one of the available Deployment Regions in the applicable Subscription Schedule, then the client data stored in Cloud Data Storage, Decision Data Storage, and Cloud file Storage will be stored in the selected Deployment Region and will not be transferred or accessed by Pega from outside the selected Deployment Region, except at the client’s instruction or in connection with a support request submitted by the client. Pega Cloud leverages multiple Deployment Regions; please review the tables to understand the regions powering your services. Pega may provide network monitoring and system provisioning activities for the Environments from its network operation centers located inside and outside of the selected region or per the subscribed support services.



Service operations and support for Pega Cloud

Service Operations and Support describes the maintenance, monitoring, support, and security locations and services we offer. Pega Support describes the client support services we offer, and Self-Service describes self-service support capabilities available to Pega Cloud clients.



Notice: This article is part of the Pega Cloud Subscription Documentation. Only the full article (not a summary) is the official contractual document.

For Pega Cloud maintenance, monitoring, support, and security locations, Pega provides Pega Cloud operations centers aligned with global privacy requirements, as per our [Privacy Notice](#).

Pega Cloud provides each client with the following Service Operations capabilities:

- **Environment monitoring and management** with proactive response to infrastructure issues and failures, resource utilization issues and tuning of Environments to support guardrail- and license-compliant applications across all client Environments.
- **Database monitoring and management** to support availability and performance for guardrail- and license-compliant applications as well as changes required by client not enabled by Pega Platform features.
- **Network monitoring and management** including firewall and security group configuration and network and system level access monitoring with 12-month storage of security audit logs.
- **Service maintenance and updates** including all scheduled Pega Platform and CRM application software updates as well as Pega Cloud infrastructure updates and upgrades.
- **Security monitoring and management** in line with the [Security Standards](#).

- **Data backup and restore management** as described in Data Backup Objectives above
- **Deployment** of new Pega Cloud Subscriptions

Pega Support

Each Pega Cloud client receives access to Pega Support, which provides follow-the-sun support through Pega's global support locations:

- North/South/Central America
- Australia
- Japan
- India
- Poland
- UK

Clients will receive premium level service for assistance with cloud issues, including:

- Problems encountered during application development
- Issues encountered during standard use or testing
- Environmental issues, including performance and configuration problems with the product
- Upgrade, or migration problems
- Other software use or operation errors

For details, please see the [Support@Pega Handbook](#).

Pega Support teams work with clients to resolve issues in the clients' Pega CloudEnvironments. Pega Cloud is contracted for using Pega business metrics (for example: users and cases) and not at the server/CPU/memory level. Therefore, it is not part of Pega's support practice for Pega Cloud support teams to share specifics of the Cloud infrastructure, such as screenshots of capacity/usage, infrastructure logs, firewall/security configurations, and details about the general architecture of Pega Cloud. The security of Pega Platform and the Pega Cloud infrastructure is a top priority



at Pega, and as part of our commitment to keep the Cloud Environments secure, Pega's practice is to not release this type of information.

Self Service

Pega Cloud provides each client with access to Self Service capabilities, including:

- The My Pega Cloud self-service portal that is available in the Pega My Support Portal
- Pega Community, which includes access to:
 - Pega Documentation
 - Pega Support Center
 - Pega Academy
- Pega Predictive Diagnostic Cloud, the Pega application performance monitoring service deployed to all client Environments.
- Pega Deployment Manager, the Pega DevOps pipeline orchestration capability
- Pega Agile Studio, the Pega Agile project management tool
- Database Management features built into the Pega Platform, including Schema Tools and Query Runner capabilities.

Service connectivity for Pega Cloud

There are a number of connectivity options that are available to connect to Pega Cloud, as well as integration services capabilities which clients may use to integrate Pega with other third-party or homegrown systems.



Notice: This article is part of the Pega Cloud Subscription Documentation. Only the full article (not a summary) is the official contractual document.

Pega Cloud offers options for connecting a client's users, enterprise and third-party systems to Pega Cloud. For additional connectivity information which is not part of the Pega Cloud Subscription Documentation, see [Pega Cloud Connectivity Options](#).



By default, client Environments are accessed via a TLS-encrypted Internet connection.

Integrations

Most clients need to integrate their Pega Platform and Pega Strategic Applications with other in-house or third-party systems. Pega provides different rule types to help facilitate integration with our clients' other enterprise systems.

Resources maintain connection properties and other configuration data for client Pega application integrations. Services are used to expose integration points into the application, such as REST APIs; and Connectors enable our clients' Pega Cloud applications to request information from external systems.

Pega Cloud includes support for multiple Application and File/Content Integration methods to support both inbound and outbound integration. A full list of currently supported Pega Cloud integration methods can be found on Pega Community.

For additional integration information which is not part of the Pega Cloud Subscription Documentation, see [Integrating Pega applications with External Systems](#).

Service level agreement for Pega Cloud

The Pega Cloud Service Level Agreement (SLA) describes the Scheduled Availability for our Production Environments.



Notice: This article is part of the Pega Cloud Subscription Documentation. Only the full article (not a summary) is the official contractual document.

The Pega Cloud production Environment Service Level Agreement (SLA) is a policy that governs the use of Pega Cloud production Environments under the terms of the Client's Pega Cloud Subscription Agreement.

Pega will use commercially reasonable efforts to make the Pega Cloud production Environment available with a Monthly Uptime Percentage of 99.95% (the service level agreement, or “SLA”), as calculated below.

$$\frac{\text{Scheduled Availability} - \text{Unavailability}}{\text{Scheduled Availability}} \times 100 = \text{Monthly Uptime Percentage}$$

Where:

- "Scheduled Availability" means the total number of minutes in the subscription month during which the production Environment is scheduled to be available, per the [Pega Cloud Maintenance Policy](#).
- "Unavailability" means the number of minutes that the production Environment was not Available.
- "Available" means the production Environment URL(s) is responding to requests.

Exclusions: Pega cannot guarantee Availability due to issues such as, but not limited to:

1. Using unsupported integrations
2. Using the service not in accordance with the documentation or Acceptable Use (see the [Acceptable Use Policy](#))
3. Exceeding the contractual entitlements under the applicable production schedule
4. Connectivity issues between client and Pega Cloud which are outside of Pega's controls

In the event that the Monthly Uptime Percentage does not meet the SLA during a subscription month, client is eligible to receive a credit equal to 10% of the subscription fees for that subscription month. Pega will apply any SLA credits against subscription fees due under the applicable production schedule in future months.

To receive an SLA credit, client must submit a written request to Pega. The request must include the dates and times of each incident of unavailability, within 30 days of the end of the subscription month in which the client alleges that the Monthly Uptime Percentage did not meet the SLA. If the Monthly Uptime Percentage is confirmed by



Pega not to have met the SLA, then Pega will issue the SLA credit to client within one billing cycle following the month in which the request is received.

Client's sole and exclusive remedy for the subscription not meeting the SLA is the receipt of the SLA credit as described in this policy. Any unavailability that is the basis for an SLA credit cannot be the basis for a future claim.

Client acknowledges that this SLA does not apply to unavailability that may result from temporary suspension of the Pega Cloud subscription in the event of a denial-of-service (DoS) attack or other external event that Pega reasonably determines may create a risk to the subscription. During such times, Pegasystems will use reasonable efforts to give the client prompt email notice of the suspension, as well as updates regarding resumption of service.

Incident response and management for Pega Cloud

Incident Management describes how Pega works to provide response and resolution for incidents that affect the Pega Cloud network and client environments.



Notice: This article is part of the Pega Cloud Subscription Documentation. Only the full article (not a summary) is the official contractual document.

Pega works to resolve incidents that affect the Pega Cloud network and client environments. Pega is committed to client satisfaction by being proactive and working to continually improve the following areas:

- Preventive safeguards in Pega Cloud Environments
- Reduction of incident occurrences
- Incident response and resolution

Pega Cloud incident response and management includes:



- A help desk that responds to client support requests, as described in the [Support@Pega Client Handbook](#).
- A web-based, mobile-enabled support request ticketing system that is used by clients and the Pega support teams for managing, tracking, monitoring, and communicating incident status from submission through resolution.
- Security monitoring capabilities which are specifically designed to concentrate on security issues.
- Pega's security and networking engineers proactively develop and implement industry-standard security practices for identity access management, data storage, and compliance to help verify the implementation of the agreed security controls for the client's Pega CloudEnvironments.
- Operations facilities replicated across the globe, which provide Environment monitoring (network, database, cloud instances, etc.) and incident response resiliency, with managed shift handovers and on-call scheduling for coverage 24 hours a day, seven days a week.
- Technical and engineering staff to provide incident response, triage, root cause analysis, and to work toward resolution. Response procedures include the use of standard operating procedures that are maintained and kept current in a knowledge base, escalation to higher-expertise tiers and supporting teams, and bridge calls for collaboration.
- Incident severity, impact, and type classification for prioritization of tickets and assignment of appropriate personnel, with supervised monitoring of ticket status and progress.
- Contingency and disaster recovery plan activation and escalation, in the event of a major incident that involves multiple clients.
- Partner and vendor incident response support (for example, for Amazon Web Services) as needed for triage and resolution.
- Reporting and analysis of incident response performance metrics to work to achieve SLAs.

Change management for Pega Cloud

Changes to Pega Cloud environments are planned, reviewed, tested, implemented, and validated to work to help protect all Environments.



Notice: This article is part of the Pega Cloud Subscription Documentation. Only the full article (not a summary) is the official contractual document.

Pega provides change management for Pega Cloud environments. Changes are planned, reviewed, tested, implemented, and validated.

Responsibilities

Pega is responsible for managing all changes to the Pega Cloud Environments, which includes the underlying cloud infrastructure, as well as patches and upgrades to Pega-licensed products. Client changes to applications that are layered on top are the client's responsibility. Client-built applications must conform to established Pega Platform best practices and Guardrail Compliance instructions that are posted on Pega Community and provided in the Pega Platform Dev Studio.

Requesting changes

To request a Pega Cloud Environment change, a client should submit a request by selecting **New Request** through [My Support Portal](#) (available 24 hours a day, seven days a week) and provide all relevant change plan information, materials, and supporting documentation. If the client has change requests for multiple Environments, please submit a separate request for each Environment. Each request must include a complete description of the change, a change plan with at least one task, and proposed start and end dates, times, and time zone. No changes can be made that are not *explicitly* listed in the request.

When submitting a Cloud Change request via My Support Portal, clients must give a minimum of two hours' notice before the change is needed. If a Cloud Change is



needed sooner – due to downtime in the Environment related to a full-system outage incident or production-impacting incident - please create a new incident or update an existing, related incident for immediate assistance from a Pega representative.

If clients elect to move private or confidential data to non-production Environments (sandbox or non-production mirror sandbox), they should be mindful of security best practices, as described in the Security Checklist (please see [Client data responsibilities Pega Cloud](#) for additional information on this Checklist).

To protect the security of Pega Cloud client information in production Environments, Pega requires written authorization from a Client Security Contact for significant changes such as access level changes, data changes, and platform changes. This written authorization must give appropriate advance notice, and must provide all detail necessary to implement the change; it is specific to one request only, and must be provided by email, document, or letter. The authorization will be attached to the Change Request as an audited record of the request. Additionally, Pega may require a signed liability release form for requests to directly access a production database. Emergency changes (such as a service outage or critical change) which require immediate response (without the advance notice) may be made with authorization from a Pega Cloud Change Manager.

Change requests should only be submitted for activities the client cannot perform through the Pega Platform Dev Studio. Changes required for the proper operation of cloud Environments or applications (configuration file changes, Pega software upgrades, and so on) do require a request submission. Similarly, change requests for non-production Environments (ex: development, test, staging, etc.) need not be reviewed by the Change Advisory Board (as they have no compliance or security impact) but should also be submitted in the change request.

Note: For each new release of the Workforce Intelligence, Process Mining, Legacy Web Chat (formerly Pega Chat), Pega Co-Browse, Digital Messaging, and Voice AI services, all client Environments are automatically updated during their maintenance windows (if applicable).



Subscription changes

To change the terms of a Pega Cloud subscription (for example, to add a new Strategic Application to the configuration), please contact a Pega Account Executive.

For additional details on Pega Cloud change management, which are not part of the Pega Cloud Subscription Documentation, see [The Change Management Process in Pega Cloud](#).

Disaster recovery for Pega Cloud

Pega provides a Pega Cloud Disaster Recovery plan.



Notice: This article is part of the Pega Cloud Subscription Documentation. Only the full article (not a summary) is the official contractual document.

Pega is committed to the preventive safeguarding of the Pega Cloud network and the high availability of Pega Cloud client instances. This commitment includes working to prevent Severity 1 incidents that could have significant business impact for Pega Cloud clients.

Pega Cloud Operations has a disaster recovery plan that is used by incident responders in the rare occurrence of a multiple-client Severity 1 incident (as defined in the plan), and which is also used to prepare the team to rapidly respond and efficiently recover service to affected Pega Cloud clients. The plan covers the following areas:

- **Physical disasters.** Pega Cloud Environments are hosted in the client's selected Deployment Region. For details on these Deployment Regions, see [Deployment regions for Pega Cloud](#). Environments, Cloud Data Storage, Cloud File Storage, and Decision Data Storage, located within the client's selected Deployment Region, are fully replicated and protected by multi-zone automatic failover. Physical disaster impacts on Pega Cloud Environments are extremely unlikely.



- **Global client support and operations facilities replication.** Pega Cloud client support facilities are also replicated and staffed in multiple global locations, using a follow-the-sun operating model. During a declared disaster situation in one location, Operations and Information Security engineers from other Pega support sites will provide monitoring, system administration, and security awareness to Pega Cloud Environments.
- **Database replication.** For client Environments, database technologies leverage state-of-the-art replication strategies, such as hot standby and real-time synchronous replication and multi-node clustering. This provides near-real-time failover for critical systems on Pega Cloud. Following recovery of service, Pega Cloud operations can perform restoration from backup, if needed.
- **Plan information.** Pega Cloud has disaster recovery plans that include roles, responsibilities, activation, response, recovery, reconstitution, and validation of Pega Cloud Environments. Pega Cloud Information Security and Pega Cloud operations regularly test these plans.
- **Prepared response.** Pega Cloud offers 24x7x365 situational awareness monitoring, and is prepared to activate disaster recovery plans with disaster recovery team response within moments of any disastrous incident. Response bridge calls would include disaster recovery responders and clients, as appropriate.
- **Announcements portal for major events.** In the event of a major incident that affects service to client Environments, Pega Cloud operations notifies affected clients (using the [My Support Portal](#) or email). Clients receive updates on restoration progress, and when normal service is restored.

For Legacy Web Chat and Pega Co-Browse, Pega relies on Regional Pairs for disaster recovery. The disaster recovery location for each Service Deployment Region is identified as a Secondary Region in the charts below. The Secondary Regions are not available as Service Deployment Regions.

Pega Co-Browse

Service Deployment Region	Secondary Region
---------------------------	------------------



USA – Northern Virginia	USA – Northern California
Ireland - Dublin	Germany - Frankfurt
Canada - Central	Canada - Central

Pega Chat

Service Deployment Region	Secondary Region
USA – Northern Virginia	USA – Northern California
Ireland - Dublin	Germany - Frankfurt
Australia - Sydney	

Data backup, data-restoration, and data durability for Pega Cloud

Pega Cloud production provides various levels of backup and redundancy for client Environment(s), Decision Data Storage, and Cloud Data Storage, to work to help provide recovery of environments in the event of service disruption or failure.



Notice: This article is part of the Pega Cloud Subscription Documentation. Only the full article (not a summary) is the official contractual document.

Pega Cloud production services provides various levels of backup and redundancy for client data, to provide recovery of environments in the event of service disruption or failure.

Pega's approach involves the concepts of both *data durability* and *data restoration*. Data durability defines our ability to keep data stored in Cloud Data Storage and Decision Data Storage consistent, while heavily mitigating the possibility of data loss when there is a failure within the data stores. Achieving data durability in this scenario is part of our native high-availability architecture. Our *data restoration* practice is leveraged when the



service must be recovered from backup, because of an unlikely and catastrophic failure within a region.

- **RPO** is the maximum amount of time during which data might be lost from Cloud Data Storage or Decision Data Storage
- **RTO** is the target time to restore the Pega Cloud Environment(s)

Data durability

Data durability provides consistency and resiliency of data when there is a failure of active resources, and high-availability processes engage to recover these critical systems. These high availability concepts include:

1. When a primary database is impacted, and the standby database must take over operation as the primary
2. When a node in a cluster is impacted, and the service must recover the failed node.

The Pega Cloud datastore that provides Cloud Data Storage uses replication services that is designed to protect data by deploying a real-time standby in a different zone and replicating the data synchronously between primary and standby. Synchronous replication means that for a transaction to be viewed as successfully committed by Pega, it must be written to both the primary and standby database. This means that committed transactions are durably written to multiple zones, heavily mitigating the potential for data loss.

Decision Data Storage leverages a multi-node clustered architecture spanning multiple zones, and a replication strategy so that a node or a zone failure does not impact the durability of data.

In the event of these failures, Pega provides a recovery point objective (RPO) of approximately 1 minute. In many scenarios, because of the strength of the replication strategy being employed, this value will be less. Automated failover and recovery of the service has a recovery time objective (RTO) of approximately 4 minutes.



Data restoration from backup

A Pega Cloud subscription includes additional data management services, such as a data backup and restore service that continuously backs up the client's Cloud Data Storage data for each Environment up to 30 days.

The Pega Cloud data backup services back up client Cloud Data Storage in all production Environments on an ongoing basis with an RPO of no more than 10 minutes in Pega Cloud. For Decision Data Storage, the RPO is 10 minutes. This is the RPO during a scenario where both the primary and standby database or the cluster have suffered an unrecoverable failure, and the service must be restored in full, from backup. These are rare catastrophic events where the capabilities in place to provide data durability described above are not viable. The time required (RTO) for a database backup restoration depends on the size of the deployed Environments.

Pega Cloud reserves the right to update these restoration projections based on improvements to existing services, new services that Pega Cloud might offer, or any changes in the support of data or regular disaster recovery testing.



Note: Backups are retained for recovery purposes only. They are not available to clients to access.

The number of monthly data restorations Pega Cloud provides depends on the supported Environment type:

- Production Environments can receive unlimited, full data restoration.
- Non-production Environments can receive up to three full database restorations per month.

Pega Cloud restores complete backups only. Pega recommends that a restoration copies backup data to the Environment type of its source. For example, Pega recommends that a backup of a production Environment be restored to a production Environment.



If the target Environment requires more storage to support the amount of data being restored, it is the client's responsibility to purchase the additional storage needed.

To request that a Pega Cloud database be restored from a prior backup, the client should open a service request through [My Support Portal](#).



Note: Workforce Intelligence, Pega Process Mining, Legacy Web Chat (formerly Pega Chat), Co-Browse, Digital Messaging, and Voice AI production Environments all provide ongoing backup for client data, to provide full restoration of services in the event of disruption or failure.

Security standards for Pega Cloud

The various security controls (technical and organizational, physical and environmental, network and infrastructure, and others) which are provided by Pega for clients' Pega Cloud Environments.



Notice: This article is part of the Pega Cloud Subscription Documentation. Only the full article (not a summary) is the official contractual document.

Pega and the client are both responsible for security in Pega Cloud:

- The Client is responsible for the security of, and access to, the Client Application at the application level.
- Pega is responsible for the security of the Client Application and Environments at the infrastructure level.



Note: For Workforce Intelligence, Pega Process Mining, Legacy Web Chat (formerly Pega Chat), Co-Browse, Digital Messaging, and Voice AI, the client is responsible for securing sensitive data that could inadvertently be shared. All these services, except for Voice AI, provide field-masking capabilities that allow

clients to mask sensitive data such as PHI or PCI, to support their own compliance strategy.

The Pega Security Program outlined in the cloud agreement governs the service on which the client Environment is built.

- This Pega Security Program infrastructure includes the hardware, software, networking, and facilities that support Pega Cloud
- Pega Cloud manages these services on behalf of each Client, from initial provisioning to final decommissioning.

Compliance

Pega provides transparency about our compliance posture on emerging and established international and local regulations and standards. Pega maintains an extensive set of compliance certifications, attestations, and third party assessments to give our clients confidence in our solutions. For details, see the [Pega Trust Center](#).

Technical and Organization Controls

The technical and organizational measures implemented by Pega include

- Encryption of personal data: Pega encrypts all data at rest in an Environment using 256-bit AES encryption. Pega Cloud-hosted web applications provide functionality for data in transit encryption with https (TLS) and digital certificates. Within the Pega Platform, Client can also use Dev Studio to configure secure TLS 1.2 connectivity to their external REST or SOAP services. (Pseudonymisation or anonymization of personal data is the sole responsibility of the Client.)
- Ability to restore availability and access to personal data: Pega shall maintain a commercially reasonable disaster recovery plan, including automatic failover to a like facility to meet the recovery point objective (RPO) and recovery time objective (RTO) parameters published in the Subscription Documentation.
- Notification of incidents: During the term of the Subscription Services, Pega will notify clients without undue delay (unless otherwise required under applicable



law) when Pega confirms any actual security incident affecting the confidentiality, integrity or availability of client data at the infrastructure layer. In the event of such a security incident, Pega will cooperate with Client in accordance with the law and regulations applicable to Pega.

- Process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures: Pega regularly reviews global industry standards for various compliance certifications, and performs high-level organizational and technical reviews at least once per calendar year, for products which are already-GA'd before the audit cycle begins. New products or services which were not GA'd before the audit cycle begins may not be included until the next review cycle. For details on Pega's trust certifications, see the [Pega Trust Center](#).
- Pega agrees to perform, or have a qualified third party perform, external penetration tests of Pega Cloud and to conduct internal network security vulnerability assessments at least quarterly. Pega shall mitigate any critical or high vulnerabilities discovered during the penetration tests or network security vulnerability assessments.

Pega is also responsible for:

- Establishing security group configurations for secure client access.
- Protecting data in transit over the Internet. This is in addition to data security protocols for which clients are responsible.
- Providing host-based virus protection services, scans, and signature updates for Pega Cloud.
- Monitoring the security of the infrastructure components in each client Environment.
- Managing the security of Pega Cloud-delivered Environments and the Pega Cloud service management systems.
- Providing a dedicated security team that manages compliance, security monitoring, and security event response.
- Accommodating requests for client penetration testing of client applications, as permitted by the Vulnerability Testing Policy.



- Subjecting sandbox Environments to hibernation to block threats and conserve energy after two hours of inactivity; Environments automatically restart when users return

Clients are responsible for the [Client data responsibilities Pega Cloud](#), as set forth in the applicable Subscription Documentation, including:

- The development, management, implementation, maintenance, and security of their Pega Cloud-based applications as they build and operate their Pega-based applications beyond the default platform. Several of these responsibilities include, but are not limited to, application and workflow development, data classification, and user administration and entitlement management.
- The security of data in transit between Pega Cloud and clients' external systems using client-selected and Pega-supported connectivity method(s) (either public Internet or private connectivity options).

Physical and Environmental controls

Pega Cloud uses third parties as its Infrastructure-as-a-Service (IaaS) providers (see supported regions for providers), which host Pega Cloud Environments in state-of-the-art, large-scale, secure data centers.

- The IAAS provides the physical and Environmental security controls for the cloud infrastructure. Pega Cloud inherits these controls as part of the shared security model . See the IAAS provider website for summary of controls available through that IAAS provider, based on your Deployment Region(s).
- Pega Cloud provides client support facilities replicated across the globe, from which Pega Cloud are monitored and maintained.
- Pega Cloud also provides security monitoring capabilities; our engineers proactively develop and implement industry-standard security practices.
- Access to the Pega Cloud support facilities is restricted to authorized personnel only. Additionally, Pega Cloud provides access controls (detailed in clients' contracts) as part of the Pega Cloud Security Program.



Access Controls

In addition to the physical security, Pega Cloud operations has implemented access control measures which:

- Restrict access to clients' Environments to only those Pega Cloud support personnel that have a documented, current business need
- Maintain a list of personnel with authorized access
- Review and approve access lists quarterly
- Remove personnel who no longer require access

All access to data centers and client Environments is logged and routinely audited.

All administration of our cloud Environments is done through a control plane, using role-based access control with multi-factor authentication.

Network and infrastructure controls

The Pega Cloud network architecture provides a level of security that allows each Client to effectively operate the Pega Platform. Pega Cloud manages and provides each client with:

- Virtual network devices to establish the boundaries, network rulesets, and access controls to govern inbound and outbound traffic in any client Environment.
- Network security controls that limit access from untrusted sources.
- Protection against distributed denial-of-service (DDoS) attacks.
- An HTTPS Internet gateway that provides access for clients who want connectivity to their Pega Cloud Environment directly from the Internet.
- Support for optional private connectivity capabilities as described in our [Pega Cloud connectivity options](#) articles. (These articles are additional Pega Cloud information which is not part of the Pega Cloud Documentation.)
- Authentication controls for Pega Cloud support personnel supporting client infrastructure. Authorized Pega Cloud engineers are required to authenticate to Pega Cloud management tools by using unique user identification credentials and



replay-resistant two-factor authentication tokens prior to being granted secure access to the Pega Cloud network.

- Continuous monitoring of the infrastructure components in each client Environment.

Malware protection

- Pega Cloud deploys anti-malware software on the Pega infrastructure level.
- Pega Cloud deploys host-based malware services, scans, and signature updates that cannot be disabled or altered by users.

Risk management

Pega Cloud security and compliance teams conduct regular audits and risk assessments of the Pega Cloud offering to maintain adequate governance over the entire Environment. In addition:

- Pega Cloud provides vulnerability and security management for Pega Cloud-delivered Environments and the Pega Cloud management systems.
- Client-led, application-level vulnerability assessment requests, which include penetration testing and other security reviews related to the client applications, can be accommodated according to the [Vulnerability testing policy for applications on Pega Cloud](#).
- At least once per year or when significant changes to the networks are made, Pega Cloud conducts an information security risk assessment on current information security controls that affect the confidentiality, integrity, and availability of client data.

Client data responsibilities Pega Cloud

The Client Data Responsibilities describe the security responsibilities which are assumed by the client for Pega Cloud Environments, including privacy & security controls, and data responsibilities.





Notice: This article is part of the Pega Cloud Subscription Documentation. Only the full article (not a summary) is the official contractual document.

Clients must agree to comply with the [Pega Cloud Acceptable Use Policy](#).

The below responsibilities will govern clients' use of the Subscription Services in addition to and in accordance with the terms of clients' Agreement and an applicable Schedule.

During the term of the Subscription Services, Client must agree to comply with the following:

Data Responsibilities

- Notify Pega of specific data domiciling or regulatory requirements, such as U.S. or EU-only data storage or Business Associate Agreements;
- Be responsible for the accuracy, integrity and legality of their content and data;
- Manage their Pega Cloud storage volume to be at or under their contracted level, through best practices including archiving, purging, or purchasing additional blocks of the type of storage needed;
- Be responsible for the classification and use of the application data they collect, including:
 - Data minimization and retention
 - Data use limitation
 - Data quality and content integrity
- Not include Protected Health Information (PHI) in a Production Environment unless using Pega Cloud HIPAA/HITECH Edition;
- Not include Personally-Identifiable Information (PII) in a Production Environment unless identified in the Schedule to the Agreement;
- Not include confidential or sensitive data in the Client Application log files;
- Acknowledge that Pega stores names and email addresses for client-identified named contacts who may contact Pega Support. If Client has regional or industry requirements that prohibit client's PII as it relates to the names and email

addresses of their staff's assigned contacts in Pega's My Support Portal (MSP), it is the Client's responsibility to register anonymous names and email address for these named contacts. It is then Client's additional responsibility to manage internal routing of these anonymous emails to their named staff.

- If Client elects to move private or confidential data to non-production environments (sandbox or non-production mirror sandbox), Client will be mindful of security best practices as described in the Security Checklist.

For additional information on accomplishing these tasks, see the below article, which is not part of the Pega Platform Subscription Documentation:

- ["Storage Types" in Understanding Pega Cloud services subscription provisioning](#)

Security Responsibilities

- Create and protect security credentials related to Client's use of the Subscription Services;
- Notify Pega within twenty-four (24) hours if it becomes aware of any actual or alleged data security incident at the application layer;
- Establish, manage, monitor, and otherwise control all application user accounts and privileges within their developed applications;
- Report issues and incidents about Pega Cloud to Pega Global Client Support, and follow up on the status of those issues to ensure that they are resolved;
- Configure appropriate security controls in their application, and monitor the security of the developed application by using Pega Platform tools;
- Configure appropriate masking for fields where customer data is private or confidential (where applicable and based on client security policies).

For additional information on accomplishing these tasks, see the below articles, which are not part of the Pega Platform Subscription Documentation:

- [Assessing your application using the Security Checklist](#)
- [The Security Checklist](#)
- Mask or hide sensitive customer information in [Configuring Pega Co-Browse](#)



- [Encrypting application data](#)

Application Responsibilities

- Be responsible for configuring a Guardrail Compliant Client Application;
- Be responsible for verifying that the application design for Client application adheres to performance best practices, by utilizing Pega Predictive Diagnostic Cloud (PDC) and adopting performance recommendations;
- Be responsible for any third-party software, tool, library or component that is installed and/or used by or on behalf of the Client in any Environment in connection with the Subscription Services;
- Be responsible for third party data flows that the Client integrates with and into the Environments;
- Agree that Pega will update Pega software within the Client's Pega Cloud Subscription Service to keep Client current on Pega's latest generally-available release;
 - Client will perform required client tasks during major and minor release updates (such as regression-testing applications) during their update window (see link below for *Pega Cloud update process* for client update-related tasks)
 - Client must be only one minor release behind the current release. Client must update to the current minor release before the next minor version of Pega Platform is released.
- For clients using the Pega Customer Decision Hub (CDH): Be responsible for adhering to Service and Data Health limits for CDH (see link below for *Service and Data Health Limits*).

For additional information on accomplishing these tasks, see the below articles, which are not part of the Pega Cloud Subscription Documentation:

- [Adding the Check guardrail compliance score task](#)
- [Utilizing Pega Predictive Diagnostic Cloud](#)
- [Pega Software Maintenance Program](#)
- [Pega Extended Support Program](#)



- [Pega Cloud Services update process for Pega Infinity release 8.4.2 and later](#)
- [Service and Data Health Limits for Pega Customer Decision Hub](#)

Layered distributed denial of service protection in Pega Cloud

Our layered distributed protection in Pega Cloud provides counterstrategies to help protect against Distributed Denial of Service (DDoS) attacks.



Notice: This article is part of the Pega Cloud Subscription Documentation. Only the full article (not a summary) is the official contractual document.

Pega Cloud provides counterstrategies to help protect against Distributed Denial of Service (DDoS) attacks.

DDoS attacks attempt to make targeted websites unavailable, thereby preventing anyone from using those websites. The attacker does this by exhausting the network's resources that would be needed to reach a specific webpage, application or its data, through sending enough false or high-volume traffic that it overwhelms the system's capability to respond. DDoS is not a security or data breach—it even denies the attacker actual access—but it prevents the use of the system and its data. DDoS is not capable of taking down the application and database servers that would be situated behind the web servers which are used as access points, nor can DDoS be used to extract or expose data.

The Pega Cloud architecture is designed to prevent and mitigate DDoS attacks in a multi-layered approach that includes but is not limited to the following areas:

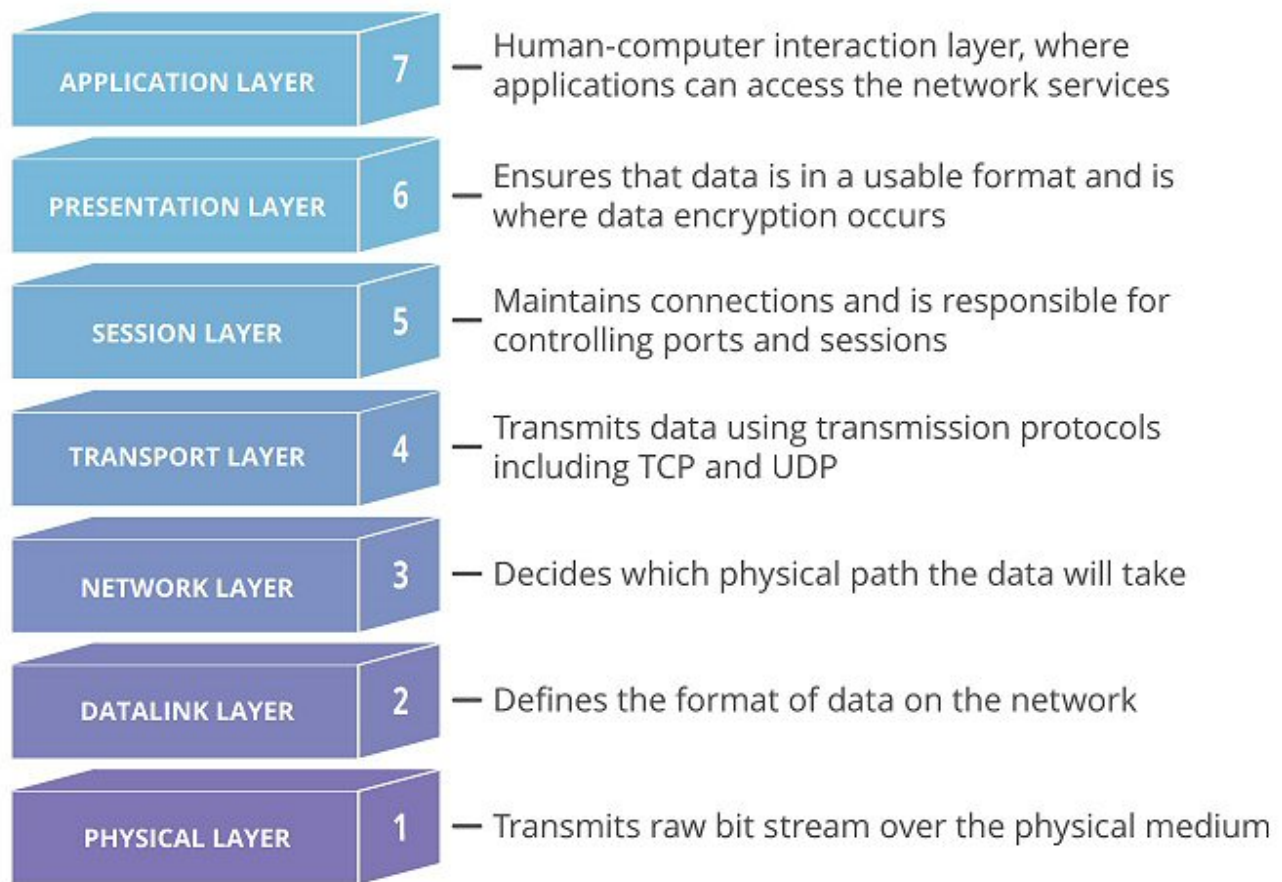
1. Scalability of Pega Cloud Environments and edge resources such as load balancers, and DNS infrastructure.
2. Edge services providing always-on detection and automatic inline mitigations that minimize application downtime and latency.



3. A web application as an application level mitigation.
4. Host based IPS.
5. Active system health and activity monitoring with selected real-time alarms.
6. Network ACLs and Firewall rules following least-privileged model to limit threat surface.
7. A client-defined allow list.

From these capabilities, the Pega Cloud service implements mitigations for the following critical areas:

- Layer 7 (application layer) attack mitigation
- Layer 6 (presentation layer - for example, TLS) attack mitigation
- Layer 4 (transport layer - for example, SYN flood) attack mitigation
- Layer 3 (network layer - for example, UDP reflection) attack mitigation
- Scaling to absorb application layer traffic
- Geographic isolation and dispersion of excess traffic and larger DDoS attacks



(Image from cloudflare.com: <https://www.cloudflare.com/learning/ddos/what-is-layer-7/>)

Based on these mechanisms and solutions, Pega Cloud provides significant DDoS mitigations.

DDoS protection is a responsibility not only of Pega Cloud, but also of the client. Pega Cloud provides a layer of DDoS protection that is—in part—also dependent on the client keeping connections to the Pega Cloud network private. Depending on clients' risk and exposure to that risk, especially if they choose to make connections available to a public or external network, they might find it beneficial to consider the services of a third party specializing in DDoS protection.

Planning for end of Pega Cloud subscription term

The clients' options as the end of the term of their subscription approaches.



Notice: This article is part of the Pega Cloud Subscription Documentation. Only the full article (not a summary) is the official contractual document.

As the end of the term of a client's subscription approaches, they have a few options. Most clients will look to renew their subscription for an additional term, in order to continue to leverage the value of their Pega deployment and potential expanded use to new areas. Some clients may elect to bring their Pega applications in-house and operate on a client-managed cloud Environment. In this way, clients can continue to leverage their investment in Pega solutions with an alternate deployment model, should they prefer.

For other clients who elect not to renew or bring Pega in-house: upon termination of the Subscription Services, and on the client's request made within 15 days of the termination date, Pega will return the client's data persisted to their Pega Cloud production Environment stored in Cloud Data Storage in a common industry-standard format such as a database export, encrypted to customary standards.

After the return of client data, Pega will delete any client data persisted to Pega Cloud. Pega follows a decommissioning standard operating procedure which relies on automation capabilities available to us from our IaaS providers. The process followed by our public IaaS providers is consistent with NIST 800-88, Guidelines for Media Sanitization. Pegasystems will notify client when decommissioning occurs via standard communication channels.

Pega does not return data for Pega Workforce Intelligence, Pega Process Mining, Legacy Web Chat (formerly Pega Chat), Pega Co-Browse, Digital Messaging, or Voice AI. Upon



termination of the Subscription Services, Pega will delete any persisted client data, using industry-recognized methods for secure erasure.

