Contents

Executive summary..................................................................................................................2
  Regulatory compliance ........................................................................................................2
  Our commitment ................................................................................................................2
Pega Application Security ......................................................................................................3
  OWASP Top 10 – 2017 .........................................................................................................3
Security features .....................................................................................................................5
  Java Enterprise Edition (JEE) ............................................................................................5
  Authentication ....................................................................................................................5
  Authorization ......................................................................................................................6
  Session management ..........................................................................................................6
  Data validation ....................................................................................................................6
  Cryptography ......................................................................................................................7
  Ciphers and keys ................................................................................................................7
  Data protection ..................................................................................................................8
  Auditing ..............................................................................................................................8
  Security alerts ....................................................................................................................8
Executive summary

The methodology and processes used by the Pega development organization ensure the development of secure applications and provide the high degree of confidence and sophisticated level of information assurance expected by end users. These aspects include:

- Engineering security training
- Developer security training
- Software development life cycles
- Mitigation of the Open Web Application Security Project (OWASP) Top 10 and other common application security risks
- Security features built into Pega products
- Security tools

Regulatory compliance

Pega Platform™ is compliant with security standards and regulations such as PCI DSS and HIPAA. It includes features such as protected data storage, data encryption, data access controls, and unique user identifiers.

Our commitment

Pega is committed to providing products that enable customers to design, build, and run secure applications with:

- A Secure Software Development Life Cycle that ensures we build secure software
- Engineering staff dedicated to application security and best practices
- Well-defined rapid response processes to address security issues quickly
- Active participation in the security community

Note: This document does not describe how to secure your application. This document is intended to give an overview of the Pega commitment to security with a review of the software and functionality available to address security for enterprise business applications within Pega software. Pega Cloud offerings and Pega Consulting Services will work with customers to derive the best security controls for their solution, but may make recommendations based on the deployment environment and compliance objectives that are operational in nature that are not reflected in this document.
Pega Application Security

OWASP Top 10 – 2017

Pega Platform enables the development of secure applications with built-in protection mechanisms and defenses against attacks and common vulnerabilities as described in the article *OWASP Top 10 – 2017: The Ten Most Critical Web Application Security Risks*.

**A1. Injection** – Multiple safeguards are provided against all injection attack types. All input data must pass through filters in Pega Platform. Specific injection flaws are addressed as follows:

- **SQL** – Built-in database access uses prepared statements with parameterized queries as well as whitelist input validation for query data supplied by the client.
- **XXE** – All XML parsers have external entity resolution disabled.
- **LDAP** – Sample and out-of-the-box rules that interface to LDAP filter user-supplied data before submitting requests.

**A2. Broken Authentication** – Pega Platform provides many control options for implementing strong authentication, such as:

- SAML SSO
- OAuth 2
- Kerberos
- Password strength policies
- Captcha
- Multi-factor authentication
- Brute force mitigation
- Operator disablement

**A3. Sensitive Data Exposure** – Strong protection must be considered for sensitive data in transit and at rest.

- **Data at rest** – There are multiple options for protecting data at rest. In addition to encryption by the data base provider, Pega Platform supports encryption of individual database columns as well. You can supply your own key or cipher options. The Pega Platform built-in encryption capability encrypts selected data using the Advanced Encrypt Standard (AES).
- **Data in transit** – Pega Platform supports transport level encryption for browser-based sessions as well as input and output REST service calls.
Pega Platform Application Security

- **Data display** – Access control polices determine user permissions for viewing data. You can perform full or partial masking of sensitive data.

**A4. XML External Entities (XXE)** – Pega Platform uses JSON instead of XML whenever possible. Where XML is still used, Pega employs both dynamic and static analysis tools and techniques to identify and correct potential vulnerabilities to XXE. Finally, our developer training courses cover this type of attack and describe how to prevent it.

**A5. Broken Access Control** – Pega Platform provides strong access control capabilities that grant user access to data objects and application functions only when needed. This is accomplished through both role-based access controls and attribute-based access controls working in tandem.

**A6. Security Misconfiguration** – Customers are encouraged to take the appropriate steps for their environment in order to make their applications more secure. Within the Designer Studio, a security checklist with over thirty items is provided for every application to help customers build secure applications. This checklist is a dynamic document that tracks the progress of securing an application.

**A7. Cross Site Scripting (XSS)** – Pega Platform performs whitelist input data validation and employs XSS filters for blocking malicious characters. Data is also filtered and encoded as necessary during output processing to disable client-side attacks. Support is provided for configuring a Content Security Policy (CSP) as well as Cross Origin Resource Sharing (CORS) policies for your application to defend against XSS.

**A8. Insecure Deserialization** – Pega Platform uses strong type checking during deserialization to mitigate this vulnerability.

**A9. Using Components with Known Vulnerabilities** – Pega performs frequent security analysis of third-party components included in Pega Platform. Commercial products that are specifically built for this purpose are used. Pega responds immediately to security issues discovered on-site in Pega Platform and provides fixes in the timeliest manner possible. Pega also encourages customers to install all of the latest patches to third-party components and to continuously monitor the security of these products to ensure their efficacy.

**A10. Insufficient Logging and Monitoring** – Pega Platform provides auditing of normal business activity as well as logging of a comprehensive set of security-related events. Included are events related to authentication, data access, and security administration. Custom event logging is also supported. Using a log aggregator and query functions, patterns of suspicious behavior are detected and acted upon.
Pega Platform Application Security

Security features

Pega Platform provides a broad range of security capabilities to prevent malicious use of, and access to, an application.

Java Enterprise Edition (JEE)

JEE specifies a set of rules to which all applications must adhere. Pega Platform is a JEE application. The JEE container in which it runs provides a certain level of security, including protected access to infrastructure components (such as databases, LDAP, and file systems), authentication and authorization, secure communications, auditing and logging, rules, failover, and fault tolerance.

Authentication

Pega Platform supports multiple types of authentication with the most common performed external to Pega Platform. Supported authentication protocols include SAML, OAuth 2, Kerberos, multifactor, Captcha, and so on. An authenticated session is required to perform critical functions in the application. Passwords or other sensitive information between the client and the application are not exchanged other than during the initial sign-on request. Failure messages do not leak sensitive information. Reauthentication after timeout accepts only the original user’s credentials. User switching is not permitted.

The built-in authentication capabilities of Pega Platform provide support for the definition of a security policy that covers a range of options. The options that are available while configuring a security policy include:

- Setting minimum password lengths
- Minimum numeric, alphabetic, and special characters required in the password
- Minimum and maximum password age
- Maximum unique historical passwords
- Number of failed login attempts before lockout
- Initial lock-out penalty in seconds
- CAPTCHA authentication settings
- Inactivity disablement
Authorization

The authorization model in Pega Platform includes both attribute-based and role-based access controls. Permission to access data objects and application functions is determined dynamically by the roles and attributes of the user. Access controls can be broadly applied to an entire class of data objects or focus on a particular field in a record. Pega Platform provides tools for the security administrator to ensure that the configuration meets requirements, for example, by running access control simulations.

Session management

Pega Platform allocates a session object on behalf of the user by using a randomly generated, unique session value to identify the session object. The session ID contains sufficient entropy (greater than 128 bits) to prevent collisions and successful guessing by attackers. It does not contain sensitive information and serves only to identify the user's session. An encrypted form of this value is included as a cookie value in HTTP responses to the client and sent to Pega Platform in all requests. Decryption occurs only by Pega Platform. The cookie is protected against client access by using the HTTPOnly security setting. Optional security features include HTTPS-only cookies as well as distinct pre- and post-authentication cookie values. The cookie value does not appear in logs or any other form where it could be used to hijack a session.

Data validation

Request processing provides several layers of protection against malicious attacks contained in input and output data. Pega Platform provides continuous protections at the server level in addition to any that are enforced by the client.

- During input processing, request data is typically assigned to application properties, which are specified to contain well-defined data types. These data types trigger server-side data validation whenever a value is assigned to a property. Data types include integer, decimal, double, DateTime, TimeOfDay, Date, TrueFalse, and others.
- Enforced length limits are applied.
- Free text input values can be configured for validation against a list of valid entries. For example, the list can be predefined during application development, or can be evaluated dynamically by using a database lookup at run time.
- Several validation rule types are available to configure on-site custom validation logic where necessary.
- A cross-site scripting filter is used during input and output processing.
Cryptography

Cryptography facilities for Pega Platform are based on the Java Cryptography Extensions API. These facilities rely on cryptography providers that are supplied by the Java JDK vendor, the Bouncy Castle JCE provider included with Pega Platform, or an alternate provider supplied by the customer. Cryptography facilities provide APIs that support both one-way and reversible encryption by using either a default Pega Platform cipher or a custom cipher.

Customers are able to supply their own ciphers or can construct an instance of a standard cipher by using a simplified textual description. Diagnostic tools are provided for discovering which capabilities are available in the Java version being used.

Note: Pegasystems does NOT provide cryptographic algorithms.

Ciphers and keys

Pega Platform provides encryption capabilities by using either the default Platform cipher or a customer-built, custom cipher as part of the standard cryptographic functions.

The Pega Platform cipher uses AES 256-bit encryption and requires no development effort to define. This cipher uses keys managed externally by the customer in key management systems, such as Amazon Web Services Key Management System (AWS KMS). Key rotation capabilities are fully supported.

A custom cipher is a cryptographic algorithm that you define. Defining a custom cipher requires you to define Java classes that implement them, and requires their installation on your Pega cluster, which requires the assistance of Pega staff for Pega Cloud customers. Choose this option if your organization has security standards that dictate the use of a cipher different from the platform cipher.
Pega Platform Application Security

Data protection

Pega Platform provides support for individual property and BLOB encryption. Data is encrypted prior to storage in the database and typically is decrypted immediately after database retrieval. Support is also provided to only decrypt on demand. Access control policies can be defined to restrict visibility of certain sensitive information by obfuscating or masking all or portions of sensitive data.

Auditing

Pega Platform audits a complete list of actions, including both successful and unsuccessful attempts to access and modify data. This auditing includes rule changes, security policy changes, log-in failures and successes, invalid data access attempts, and so on. Support is also provided for custom-defined auditing. Logged data can be aggregated and used to detect patterns of suspicious behavior.

Security alerts

Pega Platform logs security alerts whenever it detects a condition representing a possible security incident. These include:

- User switching attempts
- Access to a restricted activity, stream, or report
- Unauthorized data access
- Session hijacking
- Cross-site request forgery (CSRF) attacks
- Injection attacks
- Content Security Policy violations
We are Pegasystems (NASDAQ: PEGA) - dedicated to streamlining business and enhancing customer engagement. Our Global 3000 customers rely on our dynamic, strategic applications to drive excellence in their sales, marketing, service, and operations. We seamlessly connect our customers with their customers across channels, in real-time.

We are dedicated to helping our clients realize exceptional customer engagement and achieve operational excellence. Our adaptive, cloud-architected applications – built on our unified Pega Platform™ – empower people with comprehensive visual tools to extend and change applications to meet strategic business needs. For more information visit us at www.pega.com.