AnswerHub Security

August 2016

ANSWERHUB SECURITY

DZone Software takes information security and privacy very seriously. Through a combination of internal controls, product features, and external security techniques, we verify the security of your data on an ongoing basis. This whitepaper provides a summary of the measures that we undertake to provide peace of mind for DZone Software customers and their users.

AnswerHub Security Features

DZone Software treats security as an integral part of the software development lifecycle (SDLC). We conduct regular security code reviews before any official release and build security and training for security into our day to day processes. This process also includes an at least annual report from a secure static code analysis tool to help provide additional insight that our manual internal reviews and external vulnerability testing did not discover.

In addition to the Secure SDLC, we have also built the following features into our products to ensure that our customers' data is secure.

- Passwords stored in a salted SHA 256-bit format
- The one-way nature of this hash means that no one including DZone Software is able to discover plain text value of the passwords.
- When using SSO – remote passwords for users are not stored in our products
- CSRF protection on all forms using a time limited and random token
- XSS protection in both output templates and input processing
- Verification of attachment magic bytes to verify that the attachment being uploaded is actually the same as its extension indicates
- Products are prevented from being embedded in Frames or an iFrame by default
- Cookies are forced to HTTP-only and Secure when running under SSL
- Fine granted access control at the group and user level per Space and for the site as a whole
- Setup a collection of Spaces with different permissions to map to your organization's specific org chart
- An extensible HTML sanitizer ensures that no invalid content is posted by users
- All actions by users are logged for retrieval later in the event of a breach or mistakes posting content into incorrect areas by users

DZone Software and Cookies

An HTTP cookie is a small piece of data sent from a website and stored in the user's web browser while the user is browsing. DZone Software recognizes that many countries have different requirements for what is stored within cookies and as such, tries to set as few cookies as possible.

Customers may set additional cookies through the use of any customizations they make. The table below outlines the cookies that are set as part of the current shipping version of our products.

NAME	PURPOSE	MAX AGE
JSESSIONID	Session cookie set by the application server.	SESSION
SPRING_SECURITY_ REMEMBER_ME_COOKIE	Long term cookie allowing users to be remembered the next time they return to a site.	30 days
TH_CSRF	Random and time limited value to protect forms from cross-site request forgery attacks.	SESSION
TH_JS_SUPPORT	Simple flag to indicate that Javascript is supported by this client and fallback to less dynamic interface if it is set to false.	SESSION

ANSWERHUB SECURITY: EUROPEAN HOSTING

Hosting in Europe

DZone Software is committed to supporting the privacy regulations of the European community. In an effort to support the broadest range of customers possible, we work with Amazon Web Services to provide two locations in Europe – one in Ireland and one in Germany. Each one supports the full range of our services, including High Availability, and all data is kept within European borders. Data center physical locations and access are strictly controlled.

Article 29 Working Party, AWS Data Processing Addendum and Model Clauses

Our hosting provider, AWS, has already obtained approval from EU data protection authorities, known as the Article 29 Working Party, of the AWS Data Processing Addendum and Model Clauses to enable transfer of data outside Europe, including to the U.S. With their EU-approved Data Processing Addendum and Model Clauses, AWS customers can continue to run their global operations using AWS in full compliance with EU law. The AWS Data Processing Addendum is available to all AWS customers that are processing personal data whether they are established in Europe or a global company operating in the European Economic Area.

The Right to Be Forgotten Law

DZone Software products attempt to collect as little personal information as possible during registration. There are only three pieces of information required during sign up to a community powered by a DZone Software product, including username, a password, and a working email address. Additional information such as a first and last name, location, age, or a custom avatar may be added to a user's profile at their own discretion.

In compliance with the right to be forgotten law, DZone Software products support deleting or renaming user accounts. By renaming a user, you can change the user's real name, the username, email address and any other custom parameters with a generic or anonymous set. Doing this allows a user the right to be forgotten while still preserving their valuable contributions to your community.

Amazon Web Services provides two locations in Europe that support the full range of our services including high availability, and all data is kept within the European borders

Single Sign-On (SSO)

During community setup, a community owner may elect to connect their sign-in to an external identity provider, also known as single sign-on (SSO). This provider may automatically populate a profile with additional profile information that users have already provided with the community owner. Community owners may also choose to enhance the core profile with additional fields that a user can optionally populate.

Additional Security Controls

Datacenter Security

All data centers (including the physical access to any such data centers) for DZone Software are managed by Amazon Web Services (AWS). AWS' data centers are state of the art, utilizing innovative architectural and engineering approaches. AWS has many years of experience in designing, constructing, and operating large-scale data centers. This experience has been applied to the AWS platform and infrastructure. AWS data centers are housed in nondescript facilities. Physical access is strictly controlled both at the perimeter and at building ingress points by professional security staff utilizing video surveillance, intrusion detection systems, and other electronic means. Authorized staff must pass two-factor authentication a minimum of two times to access data center floors. All visitors and contractors are required to present identification and are signed in and continually escorted by authorized staff.

AWS only provides data center access and information to employees and contractors who have a legitimate business need for such privileges. When an employee no longer has a business need for these privileges, his or her access is immediately revoked, even if they continue to be an employee of Amazon or Amazon Web Services. All physical access to data centers by AWS employees is logged and audited routinely.

AWS operates its data centers in such a way as to be compliant with a number of global certifications including ISO 27001, PCI DSS Level 1, and the EU Data Protection Directive. For more information, please see here: aws.amazon.com/compliance

Infrastructure Security

In addition to the application and data center specific security features mentioned above, DZone Software takes a number of precautions at the infrastructure layer to ensure that data is kept secure. These precautions include:

- **Single Tenancy:** All production installations receive their own application servers and database servers. Each customer is isolated by a customer specific firewall.
- **Encryption at Rest:** Database and instance storage can be encrypted at rest if requested during customer signing.
- **Encryption in Transit:** Optional SSL when using vanity domains with customer specific certificates allowed
  - *Only TLS, No SSLv2 or SSLv3*
- **Isolation of networks:**
  - *No direct access to database servers from Internet is allowed*
  - *Front end applications are isolated from utilities such as DNS and SMTP*
- **Firewalls:** Isolated, per-customer firewalls allow only relevant ports such as port 80 (HTTP) and port 443 (HTTPS)
- **Simplicity:** Only necessary services and software are installed
- **Console Access:** Administrator access to all cloud consoles is limited to authorized personnel

ANSWERHUB SECURITY: ADVANCED SECURITY + INCIDENT RESPONSE

Penetration Testing

DZone Software performs regular security reviews, including audits of our infrastructure security and firewall rules, security code reviews (including Static Code Analysis), and web and application security penetration tests via automated and manual methods.

DZone Software also welcomes responsible security testing from our customers and many customers choose to perform their own independent audits and testing of their installations annually. If you would like to perform testing on your customer instance, please contact your dedicated customer care representative.

Employee Policy and Access

DZone Software chooses its new hires carefully to fit our core values and to ensure the security of our customers' data. Background checks, NDA, and our corporate security policy must be acknowledged upon hire and access to customer systems requires a probationary period of at least one month. Access to any system is revoked immediately when an employee leaves the company.

Production server access is strictly limited to a minimum number of employees, specifically those with a business need only, and utilizes SSH keys and secure VPN access. Additionally, access to management consoles and firewall configuration requires two-factor authentication and strong passwords.

Access to source code, utility scripts and configurations is granted through explicit approval by management.

Incident Response

The DZone Software incident response plan involves four steps – Detection, Analysis, Response, and Post-Mortem.

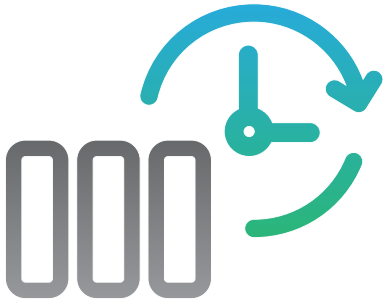
- **Detection** – the detection phase involves monitoring of systems, security alerts, vulnerability scanning, security code reviews, and penetration testing to detect security incidents.
- **Analysis** – the verification phase involves a multi-faceted analysis and prioritization of detected security events.
- **Response** – the response phase includes response based on the prioritization. This phase may contain early notification to affected customers, updates to customer sites, and any applicable bug bounties.
- **Post-Mortem** – the last step in the process involves recovery and lessons learned to prevent similar issues in the future.

The incident response process is tested at least once a year. During the Response phase, there are provisions in case of a breach involving customer or personal data.

ANSWERHUB SECURITY: BACKUP + CONTACT

Backup and Disaster Recovery

Many of the low level components that make up the DZone Software production infrastructure are provided by Amazon Web Services and are designed with multiple redundancies for maximum uptime.



In addition, critical systems such as DNS, load balancers and backups are run in a redundant manner across multiple data centers. At the database layer, all data is replicated in real time to a second master database. Snapshots are taken nightly and kept for 7 days and point in time rollbacks are available to any point in that time window. Additionally, regular backups are made of both databases and customer specific files and stored in an off-site backup.

The DZone Software Disaster Recovery plan is updated at least annually and tested at least once a year.

Contact DZone Software

- **For privacy related questions**, please email privacy@dzonesoftware.com or view our privacy policy at dzonesoftware.com/privacy
- **For security related questions**, please email security@dzonesoftware.com. Please be sure that enough detail of any vulnerability is included. A reply will be given based our Incident Response plan shown above.
- If you are a customer and have a **support inquiry**, please file a support ticket at dzonedev.atlassian.net/servicedesk/customer/portal/1 or post a question into your area in our **Success Portal** at success.answerhub.com
- **For sales and other general inquiries**, please contact your Customer Care Representative or visit our website at dzonesoftware.com

About DZone Software

DZone, the knowledge-sharing company, provides enterprise organizations with knowledge-sharing solutions, tools, and services. DZone's knowledge-driven support and knowledge-driven productivity tools are used by leading organizations eBay, GE, IBM, LinkedIn, and more.

Corporate Headquarters
150 Preston Executive Drive
Cary, NC 27513 USA
+1.919.238.7100
info@dzonesoftware.com