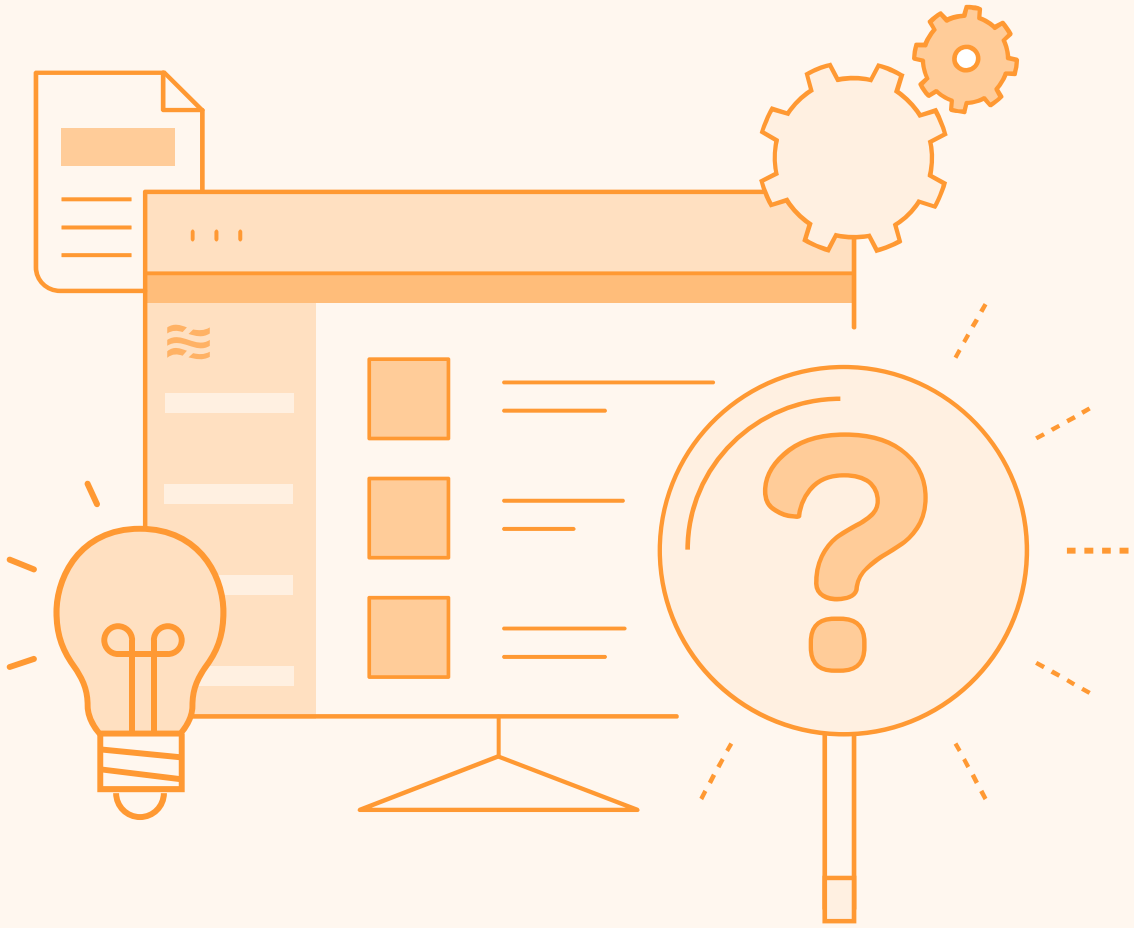
squelch



Squelch Security and Data Brief

Updated October 2018

Authentication

How does Squelch handle single sign-on (SSO)?

Squelch supports SSO Providers such as Box and JIRA. After an admin connects a provider, it appears in the console as a source. Users enter their native credentials when they select a source. Connections occur using fully authenticated API calls.

How are user credentials stored?

Squelch stores user credentials as signed OAuth tokens in secure, encrypted Amazon Relational Database Service (RDS) volumes. Squelch also applies complete tenant isolation to further protect your data. Passwords are encrypted using bcrypt. Unique session tokens protect user sessions and are verified during each transaction.

Can other Squelch users see my private content?

Squelch only indexes information that is shared by at least two users. Any private note or comment will not be collected or provided as a query result.

Security

How do you ensure information is passed securely from connected Providers or your corporate servers to Squelch?

Squelch uses the latest transport layer security (TLS) protocols and content-provider APIs to securely transport information between the Squelch cloud, corporate servers, and Providers. Also, Providers sign and approve our applications following extensive security- and quality-review processes.

Squelch connects to on-premise JIRA and Confluence deployments via a proxy that securely connects back to an authenticated tenant instance on the Squelch cloud using a tenant-specific certificate. All connections managed by the Squelch agent are protected by TLS v1.2 encoded using 4096-bit keys and both client and server certificate checks protect against man-in-the-middle attacks such as DNS or IP spoofing. The agent can only connect directly to the Squelch cloud API endpoint (*mytenant.squelch.io*) and does not house any permanent data that can be attacked or stolen.

Is Squelch certified under the EU-US Privacy Shield Framework?

Yes, Squelch was certified in 2017 and renews annually.

Do you have a formal patch-management program that proactively deploys security updates?

Yes, this is a designated responsibility of the DevOps team.

Do you harden all infrastructure such that any unnecessary services are disabled, all unnecessary ports are blocked, and insecure services such as HTTP, FTP, and Telnet are disabled?

Yes. Squelch NGINX configurations only open specific ports and URLs that are required for Squelch to perform its service. All other traffic is completely blocked. Our hosted servers do not offer direct access.

How long do you retain security logs that include timestamp source and destination IP address, hostname, user or account name?

Squelch stores such information for a month at this time.

Do you have a formal backup and recovery plan that is regularly tested?

Squelch uses Atlassian and AWS both of which have their own recovery plans.

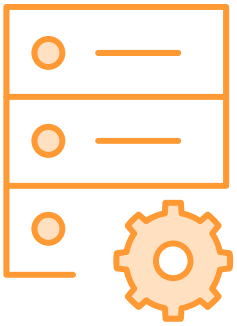
Will you return all customer information in a mutually agreed upon format within 30 days upon termination or cancelation of the subscription and/or securely destroy the data in accordance with NIST SP 800-88r1?

Yes, as stated in our Terms of Service. Deleting a Squelch tenant automatically purges any and all customer data.

Do you restrict administrator or root access to individuals requiring high-level access in order to perform their job duties?

Yes, Access to customer data, application code, administrative tenant is restricted to authorized personnel and is only possible via secured encrypted VPN tunnels.

Data Handling



Is the data encrypted on your servers?

All data within Squelch is stored on encrypted drives. Encryption keys are stored in a repository with access restricted to authorized personnel.

There are two types of data that Squelch stores.

- One type is the actual information that Squelch indexes and uses to provide results to your agents in real-time. This information is indexed in Elasticsearch on SSD encrypted volumes. In addition, Squelch uses encrypted root devices on all of its hosts.
- The other type of data Squelch stores are user credentials, or the information needed for Squelch to know what information a specific user has access to. Squelch stores user credentials on RDS encrypted volumes in Amazon Cloud Services. OAuth tokens are also signed by Squelch to ensure they cannot be used by any other applications.

On top of that, Squelch uses a tenant-based complete data isolation model to further protect your information.

How secure is your repository?

Squelch uses gold standard security practices to protect the information that it indexes from malicious access. It also relies on state-of-the-art AWS security protections from their US data centers. Our entire business model depends on it.

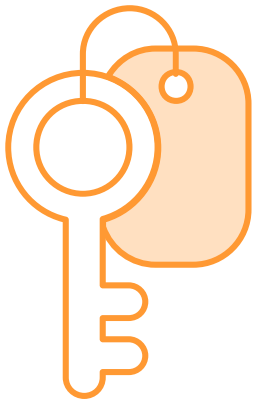
How long do you keep data on your servers?

How long Squelch keeps an indexed and organized view of your information is totally up to you. We do not store data that you have not authorized us to keep.

If you would like to remove data from the Squelch server, you can disconnect a Content Provider or remove a document. At the next collection cycle, the Data Source for this Provider will disappear for all users in the instance. If the Squelch site license is canceled and the instance is deleted, all data collected through it is deleted as well.

Data collected for reports are kept for 30 days at this time.

Permissions



How are permissions maintained?

Squelch passes through native permissions to determine access to information on a per-user basis. Whatever permissions a user has with the Content Provider is what Squelch will apply as it determines the sets of results it can display to a user. In short, if a user can see a document in its original habitat, the user will be able to see this document listed as part of a result set on Squelch.

How much work is required to ensure that the set of permissions remain current?

No work is required in Squelch from an administrator. All this control is at the Content Provider level or your own corporate infrastructure. Squelch will pick up any changes you wish to make in these environments. This may mean, however, that a user is forced to log in again if they have chosen to modify their credentials for a given Data Source. Squelch will no longer authorize access based on an obsolete set of credentials.