Squiz Connect

Security Whitepaper

Document Version

Version	Date	Author	Rationale	Reviewer
3.0	November 2023	Carrie Han	Update Data Sovereignty	Martin Pretorius
2.1	March 2023	Carrie Han	Add ISO	Martin Pretorius
2.0	December 2022	Martin Pretorius/Carrie Han	Add Data Sovereignty	Carrie Han
1.2	May 2022	C Han / M Gough / N Connell	Update of external link	Martin Pretorius
1.1	December 2021	Carrie Han / Micky Gough	Update of external link	Niamh Connell
1.0	January 2021	Carrie Han / Micky Gough	Final draft	Niamh Connell

Introduction

Cloud integration is a game-changer. It has revolutionised the way businesses approach integration and is a new and effective weapon in the battle against data silos. Despite the obvious appeal of cloud integration technologies - flexibility, scalability, and reduced time to market - there are legitimate questions to be answered about data security, platform reliability, and staff and customer privacy.

Integration platforms have extra challenges. As well as maintaining confidentiality, integrity, and availability of the platform and integration management interface, careful attention must be paid to how the data that passes through the integration system is handled.

The paper details the approach that Squiz Connect takes to ensure the security needs of the Squiz Connect integration platform, and how the security of data that passes through the system is ensured.

Access Control

Squiz Connect uses comprehensive user roles to ensure that system access is granted only to legitimate users. These comprehensive user roles provide fine-grained control over the access of each user to integrations and data.

Authentication

Squiz Connect uses industry standard strong hashing (salted SHA512 with salt) to protect passwords. Hashing is a one-way algorithm that ensures user passwords are stored in a format that cannot be easily decrypted. The additional “salt” protection prevents attackers using precomputed hash tables.

To protect against easily guessed passwords that might be used in a dictionary attack, Squiz Connect enforces a password complexity policy that prevents short or simple passwords. Additionally, the platform also supports Single Sign-On using OpenID standard technology provided by Google Cloud Platform.

User Roles and Permissions

The Squiz Connect Workspace and Member features provides organisation administrators with fine-grained control over their users’ access rights within Squiz connect.

It's important to note that users within Squiz Connect must supply their own credentials to access integration endpoints. There is no inherited privileged or shared access to applications. User access to remote systems is limited by the scope and privileges of their access to the integration endpoint.

Once an integration is configured, it will use the credentials it has been configured with, with the scope and privileges of the configured account. Consequently, it's important to ensure that the principle of least privilege is used when configuring integrations.

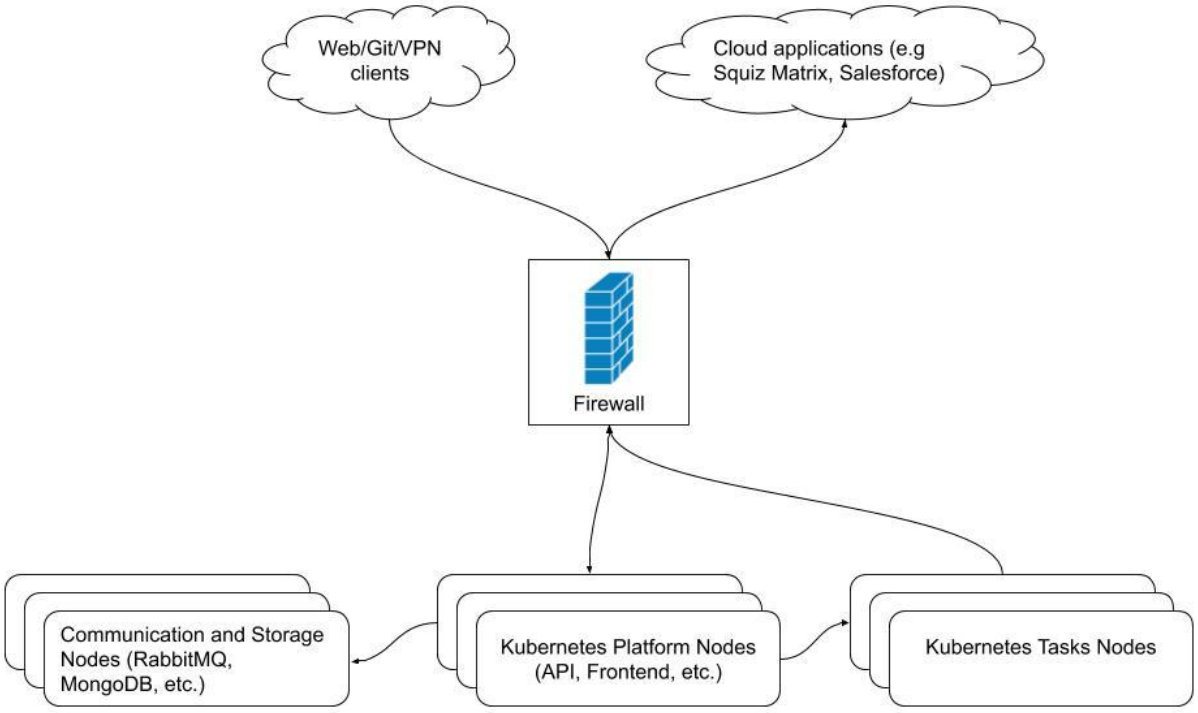
Platform Access

Squiz Connect platform is protected by strong (256 bit AES) TLS encryption. HTTPS is forced for all user and data integration traffic to provide end-to-end protection against unauthorised interception, modification, and spoofing.

Network Security

In addition to the end-to-end encryption provided by Squiz Connect, data is protected while it flows through Connect.

Squiz Connect uses a multi-tier network architecture. Inbound connections from the public Internet pass through a Web Application Firewall (WAF). Everything behind the WAF uses internal, unrouteable subnet addresses so no direct external access is possible. All data transferred through the integration environment is encrypted. Network controls between each subnet restrict traffic to allowed systems, protocols and ports. The following is a diagram that shows the overall architecture and data flows:



Cloud Applications

Only secure protocols (typically HTTPS) are used to access all external integrations from the Squiz Connect platform.

System Management

Logging and Monitoring

Squiz Connect provides monitoring, logging, and management of the overall system while maintaining the security of processed data.

Application Level Logs

Squiz Connect is a pass-through integration platform based on message queues. Transaction data may be stored temporarily for up to 30 days in the encrypted database in the case of transmission or processing errors at an integration endpoint solely to provide the ability to retry the integration until the error is rectified. The data is removed as soon as the error is recovered or 30 days has passed. Transaction integrity is safeguarded by timestamps and versioning of flows, to ensure that transactions are processed in the sequence they were requested.

Records of transactions that pass through Squiz Connect are logged to to allow for monitoring, statistical analysis, and troubleshooting.

They are stored in MongoDB and ClickHouse databases and accessed via an API frontend on the execution page to allow for rapid identification of logs in a troubleshooting scenario.

Default / recommended logging

Logging is proactively designed to ensure that logs can only contain data that a component is explicitly configured to log, i.e. endpoints, URIs and the IDs of manipulated objects. Because data security is a fundamental consideration, neither integration credentials nor the content of data involved in a transaction are logged.

By default the following information is captured in the logs when flows executed:

- FATAL log – Indicates severe errors that can cause the application to terminate.

- ERROR log – Indicates serious errors that might allow the application to continue running.
- WARN log– Indicates situations that might have an adverse performance implication.
- INFO log - Platform specific information indicates informational events output from a step of a flow such as unique identifiers of manipulated objects and the action performed on that object. (e.g. Update, Create, etc)
- Other metadata on data manipulated (size of files moved through flows, etc)
- Information about starting and stopping a container during the execution of the flow

Troubleshooting

Trace and Debug logging levels can be activated manually for troubleshooting purposes. When these logging levels are active, data passing through the flow may be included in the logs. Logging levels are set at a granular level so that data is only logged for the step reporting errors in order to minimise risk. Only users with edit access to the integration can change the logging levels.

Platform Level Logs

Squiz Connect maintains extensive internal logging and monitoring on its platform, including logins, login attempts, and privileged actions. Logs are consolidated into a centralized secure storage and are encrypted at rest for support and maintenance purposes only.

The following information are captured and stored in Graylog:

- External and internal HTTP requests with request and response-related info
- Service-specific logs for monitoring and debugging that can include different kinds of data, e.g. action name + incoming parameters

Server Hardening

Servers used in the Squiz Connect Service are hardened in accordance with Center for Internet Security (CIS) benchmarks. Operating systems are configured for auto-update.

Squiz Connect uses vulnerability management tools to scan for necessary updates to infrastructure software. Security patches are applied regularly.

Credential Management

Where Squiz Connect flows require user-supplied credentials to connect to remote systems, strong AES-256 encryption is used to protect those credentials. Alternatively, integrations can be configured to use OAuth2.

Data Security

In a multi-tenant environment, it is essential to guard against any leakage of data from one user or organization to another. Squiz Connect ensures that each user's data is private and visible only to authorised parties.

Data Privacy

While users of the Squiz Connect platform share some common infrastructure, a strong layer of privacy is enforced.

Each step of a Squiz Connect integration flow runs in a Linux container (a container is a lightweight virtual machine) which is created for the sole purpose of executing a single flow step for a single customer. These containers are isolated from one another and the hardware layer. Container filesystem access is restricted to a particular directory specific to the user and containers cannot access other areas of the filesystem. Communication between containers is tightly controlled via message queues.

At the database layer, Logical segmentation is employed to ensure that user data is not accessible to other users.

Where flows and recipes are shared between users, any sensitive data is stripped out before another user is given access to a shared recipe flow.

Squiz has a privacy policy, which further details the steps we take to protect clients' information.

Data Protection

Data “at rest” in Squiz Connect is encrypted using AES-256. While securing network links and restricting access to authenticated users prevents unauthorized access to stored data, encryption adds an extra layer of protection. Keys are managed by Google Cloud Platform and are rotated at least annually.

Data Exposure

After a flow has been tested it can be transferred to a “Production” workspace on Squiz Connect. The customer retains full control over access to this workspace. Only users who have been explicitly invited can join it. The customer can add the credentials for their cloud system within each workspace. Customers have full control over what any Squiz staff member has access to. For sensitive integrations, Squiz Connect has a powerful permissions feature to ensure that our professional services teams (or technical teams in the customer’s organisation) can build integrations without accessing real data or handling credentials for live systems.

For example, if building a flow to connect Workplace to a payroll system, Squiz can build the flow in a “staging” workspace in the Squiz Connect, and connect to a sandbox payroll environment. Once testing has completed, the flow can be deployed to the “production” workspace and credentials for the production payroll system can be added by a user (for example, the HR administrator) without any requirement for technical training or ability.

Data Retention

No data from third party applications is stored persistently on Squiz Connect, although it may be stored temporarily in the event that an error state is identified (more on that below).

Every time a flow is executed, data is brought into the platform, transformed and actioned. When the flow is finished executing all data is deleted. After each flow step, data not required by the next step is deleted unless the Squiz Connect user explicitly chooses otherwise.

If an error occurs in the execution of a flow, all data in the flow at that moment is queued on a temporary basis while the platform “retries”. The data is deleted as usual when the flow is retried successfully.

In a worst case scenario where a flow fails repeatedly, it is stopped. The data being processed at that time is stored to give the Squiz Connect user time to fix the issues without data loss. There are 2 possible outcomes:

- The user fixes the problem and restarts the flow. The data is deleted automatically when the flow has been executed successfully.
- The flow is not fixed and the data is deleted automatically after 4 weeks, with attachments deleted after 72 hours.

Data Sovereignty

Squiz Connect uses Google Public Cloud (GCP) in the us-east4 hosted in the United States for the US tenant and australia-south-east hosted in Australia for the AU tenant. Tenants are separate instances or environments of the platform. Squiz customers are using only one of these tenants in a single location. This means they are operating within either the US or AU tenant for their integration needs. This data is neither stored or transferred to other locations or transferred between the US and AU locations beyond what is described in the design and purpose of the solution. The service uses the chosen single location to process the data, and does not store any data at this location other than using it for error correction as previously stated.

Hosting and physical security

Squiz Connect services are hosted on the Google Cloud Platform (GCP). Google maintains numerous industry standard certifications and high standards of physical security. Further information on GCP security can be found at Google Cloud.

Security at Squiz

Squiz Hosting services and Support operations are ISO27001 certified, and actively maintain a proactive information risk management and security posture.

Squiz staff undergo background checks as a condition of employment. Staff are required to comply with company security policies as a condition of employment, and are bound by a Non-Disclosure obligation ensuring the protection of sensitive corporate and customer data.

Access to systems and applications is granted on a “least privilege” basis, and access is reviewed regularly. Access to production systems containing customer data is limited to a small number of senior technical staff. All application access is removed within 24 hours of employee termination.

Development Best Practices

The following processes are followed when developing platform and component features:

- Risk identification, assessment, management and monitoring
- Code review
- Third-party dependency vulnerability management
- Peer review
- Manual and automated tests
- RBAC for critical internal services

- Separated environments (development, staging, production)
- Version management (libraries, software, etc.) to prevent unexpected side-effects from updates
- Records of all published versions of a component
- Changelogs

High Availability, Backup and Disaster Recovery

Squiz Connect maintains its cloud infrastructure in multiple redundant Availability Zones, with automated failover of application services in the event that an individual server or an entire zone becomes unavailable.

Database are continuously replicated to a hot spare. If the primary database becomes unavailable, traffic can be directed to the secondary system with minimal recovery time objective and without loss of data.

Squiz Connect also maintains backups of its operational systems (daily full backups). Backups are stored in secure encrypted storage, and restoration is tested regularly.

Squiz Connect has maintained high uptime for its service. Squiz Connect systems are continuously monitored and clients are notified of any incidents that may affect availability.

Performance

To provide high performance and scalability, Squiz Connect uses a pool of workers. Events are generated in the system either by polling or by asynchronous event triggers (webhooks). Polling is done by an expandable pool of polling workers.

Squiz Connect does not impose any design limit on total data volume or number of transactions. Squiz Connect can handle very large data volumes and million of trigger events per day.

Squiz conducts platform testing, and has tested synchronisation of a very large number of trigger actions from a 3rd party ticketing system. The trigger events were delivered via inbound webhooks. During testing, Squiz Connect handled more than 1.2m inbound webhook events per flow per day, over 50k inbound events per hour!

Incident Response

Squiz maintains a Security Incident Response Plan which details responsibilities and procedures in case of a security event, including attempted as well as actual compromise of our systems. The Security Incident Response Plan is regularly tested for completeness and effectiveness by the Squiz support and hosting teams.

In the event of a breach involving exposure of customer data, the Squiz Support team will promptly notify affected customers immediately after incident verification.

Auditing, Testing and Certification

Squiz Connect has achieved SOC 2 Level 1 compliance for its cloud-based services. This involves a comprehensive examination of security and privacy practices, as well as the reliability and availability of the service. The Squiz Connect cloud application has also undergone other external security audits, for example as part of Salesforce and Google suite app certifications. In addition, internal testing and vulnerability analysis is performed on an ongoing basis, as well as periodic penetration tests performed by a qualified 3rd party firm.

After conducting thorough due diligence on the vendor, we have verified that the platform vendor's development practices and operations for the Squiz Connect solution conform to internationally recognized best practices. Based on Squiz's certification against ISO27001, we can affirm that both the Solution and our implementation of it, as well as the GPC, have all been certified against this standard.

-- End --