A Quiq white paper

Enterprise Agentic AI for CX Platform

Security Overview

Quiq's AI for CX platform is trusted by many companies - Fortune 100 to startups. Security is key in everything we do. The Quiq team has extensive experience building applications that meet the security, reliability, and scalability of the most demanding enterprises.

This document is intended to introduce Quiq's security policies and practices. We are available to answer additional questions via email support@quiq.com Our security team is reachable at security@quiq.com for urgent security concerns.

Security at Quiq.

Quiq is a security-first company, building security into all of our products from conception through deployment. Our security posture is based on Defense in Depth and Zero Trust principles. In addition to training all of our employees on the importance of security and new threats, we have a security team who ensures security practices are followed throughout the development lifecycle. The security team is led by our Chief Information Security Officer, who meets with the executive team on a regular basis to discuss security concerns.

Compliance.

SOC 2.
Quiq's SOC 2, Type II compliance audit was completed in September 2024 with no exceptions. This audit covered the period October 1, 2023 - September 30, 2024

Health Insurance Portability Act (HIPAA).
Quiq may enter into a Business Associate Agreement (BAA) with organizations that are Covered Entities with obligations to safeguard Protected Health Information (PHI). If your use case involves PHI, please work with your Quiq Account Executive to initiate the BAA process.

People Security.

At Quiq, we recognize that security starts with the people who create the product. All employees and contractors must read and acknowledge a Non Disclosure Agreement, Code of Conduct, and Information Security Policy Manual.

Credentials and system access are promptly removed when an employee leaves or changes job functions. Access is granted as-needed, with approval from senior management.

Security Training.

All new employees must review our security documents and practices. In addition, the Security Team continuously monitors and identifies new threats, including phishing awareness campaigns, and publishes that information to all employees as required reading. Finally, all employees must attend our annual security training, and engineers must additionally attend annual secure code training.

Background Checks.

All candidates and contractors must pass stringent background checks by a specialized third-party before starting employment at Quiq. For U.S. employees, these checks include: SSN validation, SSN address locator, National Criminal History, National Sex Offender Registry, and Statewide Criminal History.

Product Security.

AI Security.

At Quiq, protecting our customers' data and privacy isn't just a policy; it's a core principle that guides everything we do. We recognize the immense value and sensitivity of your data, which is why we're committed to its protection above all. In the rapidly evolving landscape of AI technology, we stand firm in our resolve to deploy only the most suitable AI tools, tailored to serve specific purposes, without compromising your privacy. Our approach to AI is one of cautious optimism: we see its potential to revolutionize customer service and operational efficiency, but we're equally aware of the need for stringent management to ensure data privacy and security.

Quiq's dedicated AI and data science team is responsible for the construction and maintenance of Quiq AI models. This team works with our internally developed generic models containing data that is not specific to your company and do not contain any of your proprietary data. For instance, our Unimportant Messages Filtering model classifies conversation closing phrases. Depending upon the Quiq features you have enabled, Quiq may also create custom AI models specifically for your Quiq tenant, derived from your proprietary data that has been thoroughly redacted and processed to eliminate personal identifiers. These AI models are meticulously calibrated to cater to the unique requirements of your business, and the AI models will be used only by your business. It is our strict policy to never share your data used in the AI Models with any other external entities for AI modeling.

Quiq also incorporates third-party Large Language Models (LLMs) into specific components of our AI products, including, but not limited to, Quiq Compose and select Quiq Agents constructed in the Quiq AI Studio. We place utmost importance on the protection of your data to reasonably ensure it is not misused for subsequent LLM training by a third-party. For example, any information exchanged with these LLM vendors is strictly prohibited from being used in future LLM model training. We collaborate exclusively with trusted and reputable vendors, as detailed on our sub-processor list. Our contractual agreements with these partners forbid the use of Quiq and our customers' data for any form of third-party training or enhancement, ensuring your data's integrity and confidentiality.

Product Security Reviews.
Security is discussed and examined by the development and security teams at each phase of the software development lifecycle: requirements, design, implementation, and deployment.

In addition to overseeing security during the product design and implementation, the security team ensures that the products in our production environments remain secure by continuously performing security activities, including:

- Internal security reviews before product launch;
- Annual penetration testing performed by third-party auditors;
- Continuous execution of internal and external security tests;
- Intrusion detection;
- File change monitoring.

Change Management.

Quiq has a formal change management process where all changes are tracked and approved. Each change is associated with the original ticket in our project management system, as well as the underlying service versions built in response to the change. The versioned services are monitored, tested, and approved as they move through our clusters: Development, Manual QA, Performance Testing, Stage, Demo, and finally Production. Quiq has a Change Management Policy and formal Software Development Lifecycle to support these processes.

Encryption in Transit.

Quiq encrypts all data in transit within our software using TLS 1.3 (falling back to TLS 1.2 when necessary). This includes data inside our firewall and all data connections in and out of the firewall. Encryption of data once it leaves Quiq and enters a messaging channel (e.g. SMS) depends on the security practices of each channel. Quiq removes credit card numbers when they enter our systems and are never stored. Our clients can also configure additional data removal patterns. Finally, all HTTPS keys are rotated at least annually.

Encryption at Rest.

Once data enters our firewall, it is always encrypted when stored in any of our data stores. Data is encrypted using 256-bit AES encryption.

Customer data is never exported to or transferred to an unencrypted device.

Tenant Data Isolation.

Quiq is a multi-tenant SaaS solution. Our production environment services many clients. Per tenant data isolation is achieved through logical segregation in the data access layer of our product architecture. This ensures that no application programmer error could inadvertently cross contaminate data between Quiq tenants.

Service-to-Service Authentication.

Quiq uses microservices for all our back-end services that reside behind our public firewall. As an added layer of security, these services authenticate using Java Web Tokens (JWT), which are signed and time stamped with a large, shared secret. Access to this secret is granted to the microservice during startup only after the service has been validated as a service we created and one that our cloud operations team explicitly started from AWS. The shared secret is stored in an encrypted vault, and only exists in the microservice's memory. All JWTs have a five minute expiration.

Account Security.

Quiq secures our customers' users passwords using industry best practices. When using our native Identity Provider, we employ bcrypt with a very large hash, and we only store the password hash for future verification. Passwords must follow the most recent NIST password recommendations, and cannot appear on the list of one million most frequently used passwords. Multi-factor authentication is supported and may be enabled at our customer's option.

Our customers may use their own IdP such as Oracle, Salesforce, Zendesk, Google, or other OAuth 2.0 based IdPs. We will authenticate against those IdPs using their best practices, including multi-factor authentication when enabled in the IdP.

Session Security.

The Quiq UI issues API requests using a signed and timestamped "access token." The token uniquely identifies the client session. The default timestamp is five minutes, after which the token is rejected. To refresh the access token, the client must issue a refresh request before the five minute expiration using a different signed and timestamped "refresh token." All tokens are validated immediately when presented to our public gateway. Invalid requests are logged and rejected. Valid requests are forwarded to the other backend services.

Penetration Testing.

At least once a year, Quiq performs third-party penetration tests and addresses all findings in a responsible timeframe based on severity and risk.

Responsible Disclosure.

Quiq appreciates and may reward the efforts of independent security researchers whose ethical hacking efforts make the internet a safer place. Quiq encourages ethical hackers to report potential issues at https://quiq.com/responsible-disclosure/.

Cloud and Network Infrastructure Security.

Infrastructure and network security are critical for the safety and trust of our customers using our platforms.

Asset Management and Ownership.

The security team continuously reviews every asset in our environments, validating its purpose, ownership, and security classification. The security team reviews and manually approves a new infrastructure asset before it can be added to our infrastructure automation. Our infrastructure creation is fully automated, ensuring environment uniformity across clusters and auditing capabilities. The security team owns and reviews these scripts.

Infrastructure Management.

Direct access to infrastructure, networks, and data is minimized to the greatest extent possible. Quiq requires 2-factor authentication on all administrator accounts associated with our infrastructure and cloud operations. Change requests are managed and executed by the security team in coordination with the cloud infrastructure team. Production systems are further restricted and exist in an entirely different AWS account and VPC from the Development/Test systems. Production access is restricted to the security team and approved members of operations and engineering.

Network and Service Monitoring.

Quiq logs high risk actions, configuration changes, and unverified modifications across our development and production clusters. We also continuously execute security and monitoring agents that identify and report operational and security anomalies. These anomalies are immediately reported to the security and development teams for prompt analysis.

Security Log Retention.

Security logs are retained for one year. Access to these logs is limited to the security and cloud operations teams.

DDoS Prevention.

Quiq uses redundant CDN providers to protect our static assets against DDoS. Our services utilize additional DDoS capabilities proved by AWS.

Server and Container Security.

Quiq uses Osquery for host based intrusion detection for all assets. Security patches are automatically installed daily. Our microservices execute within read-only and signed Docker containers. All Docker containers have been configured to execute using a non-root account, and employ Alpine Linux to further reduce their surface area.

Employee Computer Security.

Anti-virus, malware detection and adware blockers are installed on all employee computers. Disk encryption is used, and security policies are centrally administered and deployed. Timely installation of operating system updates is monitored and enforced.

Incident Response Program.

Quiq has an Incident Response Policy and Plan. The Incident Response Plan includes response plans for all plausible threats and scenarios. The response plans are reviewed at least annually. The Security Incident Response Team assesses the threat of all relevant vulnerabilities or security incidents, and establishes remediation and mitigation actions for all events.

Server and Data Backups.

Quiq performs regular backups of account information, machine images, message records, and other critical data using Amazon S3 cloud storage. All backups are encrypted in transit and at rest using strong encryption. Backups are stored across multiple availability zones and AWS regions for redundancy. Backups are kept for one year.

Physical Security.

Datacenter Physical Security.

All of our servers reside in AWS or Azure data centers. Quiq staff accesses these machines using a VPN with hardware based 2-factor authentication. For AWS security, please see https://aws.amazon.com/security/.

Office Location Security.

All laptops are encrypted, and access to corporate servers and resources require 2-factor VPN access, even within the office network. The physical servers reside in AWS data centers.

Third-Party Security.

Quiq uses third party solutions when it is cost effective and there is a strong business case to do so. Third party sub-processors are disclosed at https://quiq.com/sub-processors/. Interested parties can sign up for notification of changes in sub-processors on that page.

Quiq has multiple applicable policies including a Vendor Management Policy and Third-party Connection Policy, all which require oversight by senior management and security teams.

Initial Security Evaluation and Onboarding.

Before incorporating any third party solution, our security team evaluates the proposed solution, validating that the third party meets our security requirements. The security team also meets with the development team to determine if any product changes, such as application level encryption, are needed to onboard the vendor. Once the vendor is chosen, the security team meets with the cloud operations team to assess how the third party will be monitored for compliance and if any scheduled, recurring audits are needed.

Termination of Contract.

Upon request, Quiq ensures that all data is returned and/or destroyed at the end of a vendor relationship.

Third-Party Security.

The Quiq team takes the trust placed in us by our customers very seriously. The security landscape changes quickly and we adapt our security posture to match. While the information contained in this document is up-to-date at the time of publication, the rapidly changing world also dictates rapid changes in our security practices. This document will be updated periodically to reflect current practices.

Security questions may be asked at support@quiq.com. Security issues should be addressed to security@quiq.com.

More information about Quiq API's and security can be found at developers.quiq.com.

Last Updated: December 27, 2024