Quinyx

Quinyx Security Overview

Building security into everything we do

September 2024

Table of Contents

Introduction

With increasing cybersecurity threats and fast growing cloud services demand, the latest technology, security solutions and infrastructure management are becoming increasingly prevalent. Companies need to rapidly innovate and scale to meet market demands. Many fast growing companies rely on Software as a Service (SaaS) suppliers to provide best-in-breed applications and specialized services. These companies benefit from industry-leading secure infrastructures and security practices that cloud service providers can offer.

Quinyx is the world's most trusted Workforce Management cloud solution provider, helping people and businesses grow. Our security-rich practices are embedded across all of our technology and processes. We are in the business of people and keeping Quinyx secure is fundamental to the nature of our business, keeping our customers' data secure is our primary security focus.

For years we've worked with our customers to keep their sensitive data, such as personal data, leave histories and pay related data safe. Each of these customers are willing to trust Quinyx with their data.This document provides an overview of our security goals, controls and how we excel in securing our customers' data and privacy. The content of this document is intended as a starting point for broader and deeper security discussions.

You might be also interested in our Data Privacy and Information Security documentation. If you have any security related questions please feel free to reach out to us.

Email us at
dataprivacy@quinyx.com

1. Our company and products

Quinyx is the leading AI-powered workforce management software that makes the complex tasks of scheduling, time reporting, communicating, budgeting and forecasting deskless workers simple. Since 2005, Quinyx has been on a mission to create a better work-life for millions of people.

Today, we help companies around the world reduce labor costs , remain compliant and improve workforce efficiency - all while boosting their bottomline, employee satisfaction and retention. Quinx's AI-powered workforce management software is the #1 WFM app on the market, reviewed by 28.000+ users and highly ranked by Capterra andG2Crowd. It includes scheduling, engagement, time & attendance, strategic planning, demand forecasting and labor optimization.

The Quinyx products are offered as Software-as-a-Service (Saas) solutions.These cloud solutions are available to customers through web and mobileapplications and as well as application programming interfaces (API's).

2. Security education and awareness

At Quinyx we have a dedicated team that educates and familiarizes our employees about security best practices. Our security program includes new employee onboarding to IT security - covering topics such as risks, basic security measures and company policies, awareness training, access to security knowledge base and security training. Our security program is mandatory and we measure attendee rate accordingly.

In addition to our security education and familiarization training we reviewand update security policies and standards annually.

3. Compliance

The Chief Information Security Officer (CISO) has the responsibility to coordinate and review the security work within Quinyx and its suppliers, and to ensure the security standard is followed within the organization. The CISO has an advisory role for the ongoing operations, has responsibility for the security work at Quinyx and follows the System Managers throughout the organizational structure. System managers ensure that guidelines are designed for security in their respective areas. This is done in consultation with CISO, who reports regularly to the management team.

The objectives of the security work at Quinyx are to ensure that the business has a risk based approach to ensure proper controls are in place to protect customer, user and employee data and that Quinyx remains compliant with any local legislation and certification including ISO 27001:2013 and GDPR.

4. Data centre and security

Quinyx is a 100% cloud based solution hosted in Amazon Web Services (AWS).With the availability of at least 2 zones, Quinyx's set up allows us to maintain high availability and support fail-tolerant architecture.

Primary regions are Frankfurt (EU) and North Virginia (US) divided over at least two availability zones per region and allowing instantaneous disaster recovery for most scenarios. Adding on yet another layer of security, secondary regions for disaster recovery are Ireland (EU) and Oregon (US).

Every internal service is active in at least two Availability Zones and load balanced using proxies. As all facilities are strategically positioned across various geographic locations, all services can handle failure of a single zone with a high level of redundancy.

Our services are scaled using Docker technology ensuring that we can scale efficiently and quickly in our cloud environment. Our storage layer is automatically scaled as well based on required load.

Quinyx has an ISMS (Information Security Management System) based on the standard ISO 27001 that provides a comprehensive framework for managing and protecting our information assets. ISO 27001 outlines the requirements for establishing, implementing, maintaining, and continually improving an ISMS. It emphasizes a risk-based approach and includes controls for information security tailored to the organization's needs. Building an ISMS on this standard demonstrates our commitment to best practices within information security management.

4.1 Customer data security

Only System Administrators are granted access to our data centers, if their job responsibility requires it. Reasons for data access include initialconfiguration, support and troubleshooting. Access rights are traceable, timelimited and follow strict approval processes.

4.1.1 Application security

Access to the application and its stored data, regardless of user role, is secured using a personal identifier such as email address or login ID and password. Data that can be utilized to access customer and user data, such as passwords, are stored in encrypted format. The customer can impose a heightened password security level on its users which requires that passwords: are at least 12 characters long (max 128 characters), containingat least two numeric and two alphabetic characters.

Access to the full data set is only given to Quinyx representatives who absolutely require it to perform their work and Quinyx routinely reviews this access to determine whether, depending on the representative’s current needs, there are grounds for revocation. All Quinyx representatives are subject to confidentiality agreements and are instructed in best practice data security procedures as part of their onboarding. All digital work environments are safeguarded with a central authentication mechanism which ensures that users only have access to data in each respective software application that is crucial to their ability to fulfill Quinyx’ agreement with the customer. The application is guarded by server side validations based on the user’s actual and stored role and access rights. Only data valid and allowed for the specified user is transmitted to the client application layer ensuring that no data is leaked by investigating the data sent out from the server environment. All communication between client software and third-party applications is encrypted using SSL using SHA-256(512 bits) with RSA encryption.

4.1.2 Block-level data

Data at rest is encrypted using mechanisms built into the hosting provider's platform with keys on an HSM (Hardware Security Module) which the provider does not have more than physical- and log-access to. EnvironmentSeparation Development, testing, staging and production environments are separated on different servers and network segments and are not connected in any logical way.

All environments listed are hosted using the same security levels as if it were a production environment. Logging of Data Changes Any changes to critical application data such as access rights, agreement templates, individual agreements, users, planning units, schedule and time punches are logged, regardless if they are performed by Quinyx representatives on behalf of the customer or by the customer's users themselves.

4.2 General security audits

On an annual basis, Quinyx invites an external security company to audit and penetration test our environments. These audits and tests are summarised in reports highlighting vulnerabilities, if any, which in such a case are addressed immediately

4.2.1 Client Protection (PC)

Quinyx is protecting all company PCs to safeguard sensitive data from cyber threats. This includes implementing robust antivirus software, firewalls, and regular updates to security protocols. Educating clients to recognize phishing attempts and practice safe browsing habits are also key components of our client protection strategies.

4.3 SSO and MFA

Quinyx enforces SSO (Single Sign-On) on most of our internal applications to simplify our employees' use of them. This allows access to multiple applications with a single set of credentials, reducing password fatigue and the risk of password-related breaches. MFA (Multi-Factor Authentication) adds an additional layer of security by requiring two or more verification factors, significantly decreasing the likelihood of unauthorized access. Combining SSO with MFA provides convenience and enhanced security for our employees.

4.4 Risk Assessment

Quinyx has a risk assessment process based on ISO 27001 and FMEA (Failure Mode and Effect Analysis), conducted yearly or when significant changes occur. The risk assessment process is a foundational element of information security. It involves identifying potential risks to information assets, evaluating their likelihood and impact, prioritizing risks, and applying appropriate controls to mitigate them.

5. Solution security

5.1 Solution security

Quinyx hosting environment is a fully redundant and scalable solution hosted in AWS hosting environment fulfilling ISO 27001 for security requirements, ISO27017 for cloud security and ISO 27018 for cloud privacy ensuring GDPR compliance. Read more about AWS hosting environment's physical security and access here.

5.2 Operating System Security

We have a conservative upgrade policy where we receive and analyze security advisories and decide whether they pose an actionable attack vector to us or our customers using the platform before upgrading. All servers are running Linux operating systems that are hardened to the usage of the specific server.

5.3 Mobile security

Access to the mobile application, in addition to the above stated ApplicationSecurity measures, is protected by both - TLS (Transport Level Security) andApplication Security. Application Security of mobile applications is based on the latest security standards for authentication and authorization of user access. Authentication rules applicable as described above in ApplicationSecurity section, and authorization is based on OAuth2 standard combined with JWT (Json Web Tokens). Any authorization details passed via network are: Digitally signed (JWS) with SHA-256 (2048 bits RSA algorithm key) And encrypted (JWE with 256 bits AES algorithm key) All of the above is in addition to protection on transport level using encryption methods stated above in Application Security section

5.4 Back up

Quinyx takes full automated backups of configuration, code and data every 3 hours to both a local storage and a secondary site. Data is also copied in real-time to a database replica on a secondary site to not lose any data in the unlikely event of a full disaster in both availability zones of the main site.This gives us a current RPO (Recovery Point Objective) of maximum 3 hours. Backups are stored for at least 30 days.

5.5 API security

One of the data channels provided by Quinyx is access through API. API access is highly secured with multiple levels of protection, including TLS(Transport Level Security), Network Security, Application Security and Security Gateways. Efficient components of such architecture guarantee a high level of customer data safety. API Security implementation is based on the latest security standards

5.5.1 API Authentication Controls

API Security requires stronger policies around the length and complexity (at least 2 times stronger) of credentials than those described above in the Application Security section. When integrating with customers, customer client (API integrator) credentials are never stored as plain text within systems of Quinyx, instead those are hashed using strong hashing techniques. This eliminates the possibility of unauthorized access from internal Quinyx systems.

5.5.2 API Authorization Controls

Strong controls around API access authorizations are in place to supportmanagement of access - so access could be efficiently enabled andrevoked when needed. API Authorization uses various techniques, includingOAuth2 standard combined with JWT (Json Web Tokens).

In this scenario the authorization details passed via network are: Digitally signed (JWS) with105.4 Back up5.5 API securitySHA-256 (2048 bits RSA algorithm key) And encrypted (JWE with 256 bits AES algorithm key) All of the above is in addition to protection on transport level using encryption methods stated above in Application Security section.

5.5.3 API Gateways

API Gateways provide an extra layer of security in combination with othermeasures, such as Network Security. API Gateways support secure routing ofauthorized traffic towards the internal services, so the internal systems ofQuinyx would not be exposed. Those also guarantee the additional protectionfor the whole API layer as such, effectively providing protection againstunexpected load (circuit breakers, throughput limits) - improving the overallstate of API layer defence mechanisms

5.6 Network security

Quinyx uses a centralised authentication mechanism for all servers includingtest environments. It is group based with minimal rights to users granted on aneed-basis.

6. Secure Development lifecycle

At Quinyx, we integrate security requirements into every stage of our softwaredevelopment cycle.All changes to the product follows a well defined Change ReleaseManagement Process which includes steps and controls for designing,implementing, testing and releasing any change.Quinyx's product delivery teams consist of cross-functional team members,each specialised in their area to ensure that changes to the product aredeveloped with adherence to risk related to impact of business priorities,technology, user experience, quality and information security.

Controls are automatically built into issue tracking and version control tools to ensure processes are followed and that each change follows the same flow from design, through development, code review, testing and deployment guaranteeing that a minimum four eyes principle is followed for each step.Testing is done on multiple levels both automatically and manually to ensure all aspects of information security and user experience are taken into consideration to limit any risk of a downgraded service. Tests are executed in multiple environments to ensure that the change can securely be deployed with regards to functional and non-functional requirements. All data used for testing is anonymised.The Release process is usually concluded by the release notes distribution, and in case of API - the API documentation is constantly maintained.Efficient routines and support channels are established to provide customers support from Quinyx. Internally, at R&D there are always multiple resources from the development team assigned to monitor those support channels.

7. Disaster Recovery and Contingency

Quinyx main hosting is shared over at least two different availability zones at the Primary site and all components of the environment has at least one instance in each availability zone. In the unlikely event of full malfunction in both availability zones at the Primary site, Quinyx will effectuate the Quinyx Disaster Recovery Process. The disaster recovery time is currently estimated to be a maximum of 24 hours.

8. Service Availability

Quinyx offers a highly redundant and scalable platform and product. Service availability is very high and is contractually guaranteed to be at least 99,5%over 24 hours 7 days a week, outside planned maintenance windows.Historical SLA is over 99.98%, even including planned maintenance.

Our support is tiered in Bronze, Silver, Gold, and Platinum, to accommodate the level of support required. The Platinum tier means 24/7 support.

All support tickets are logged in the ticket handling system and closely monitored and handled by our support team, and also by our RnD-team.

There are named contact persons on the customers side. This is to ensure that only people, approved by the customer, can access the full set of data, and that only fully Quinyx-trained people can discuss any configuration changes with the support.

Quinyx has a 1st line, and a 2nd line support, and depending on the complexity of the case, the right team is involved. Also there is incident management in place, with clear responsibilities, and robust processes.Support is given fully in Swedish, English and German, however the team understands many other languages, but replies are given in the above mentioned languages.

9. Whistleblowing and Information Security

Quinyx has a whistleblowing function that plays a crucial role in information security by providing a mechanism for employees and externals to report unethical or illegal activities within our organization. It is essential for maintaining transparency and accountability to our customers, partners, and employees.

Disclaimer

Statements in this paper are non-binding, as-is, and for informational purposes only. Because our security procedures and policies change over time, we cannot guarantee that information will remain the same over time.