unqork

Unqork Platform Security

Inside the process and controls that define Unqork's security-first SaaS

Contents

Security is an essential part of any SaaS offering. In today's digital world, cyberattack prevention and the protection of sensitive data have never been more paramount. To meet the digital requirements of the modern enterprise, Unqork leverages stringent controls and protocols to deliver a multitiered defense you can trust. We take a robust People, Process, and Technology approach to provide a platform that protects you and your customers.

Unqork's vigorous security measures are compliant with both commercial and federal industry standards. Our team has decades of collective experience in some of the world's most complex and demanding sectors such as finance, insurance, government, and healthcare. We understand security and compliance challenges faced by large organizations and are here to help you overcome them.

Enterprise security is at the core of Unqork's platform—and our organization. Indeed, Unqork hired a security officer before we even hired our first engineer. And since then, our security team and our capabilities continue to expand and evolve. In this guide, we will provide an overview of how we've elevated Unqork platform security from top to bottom.

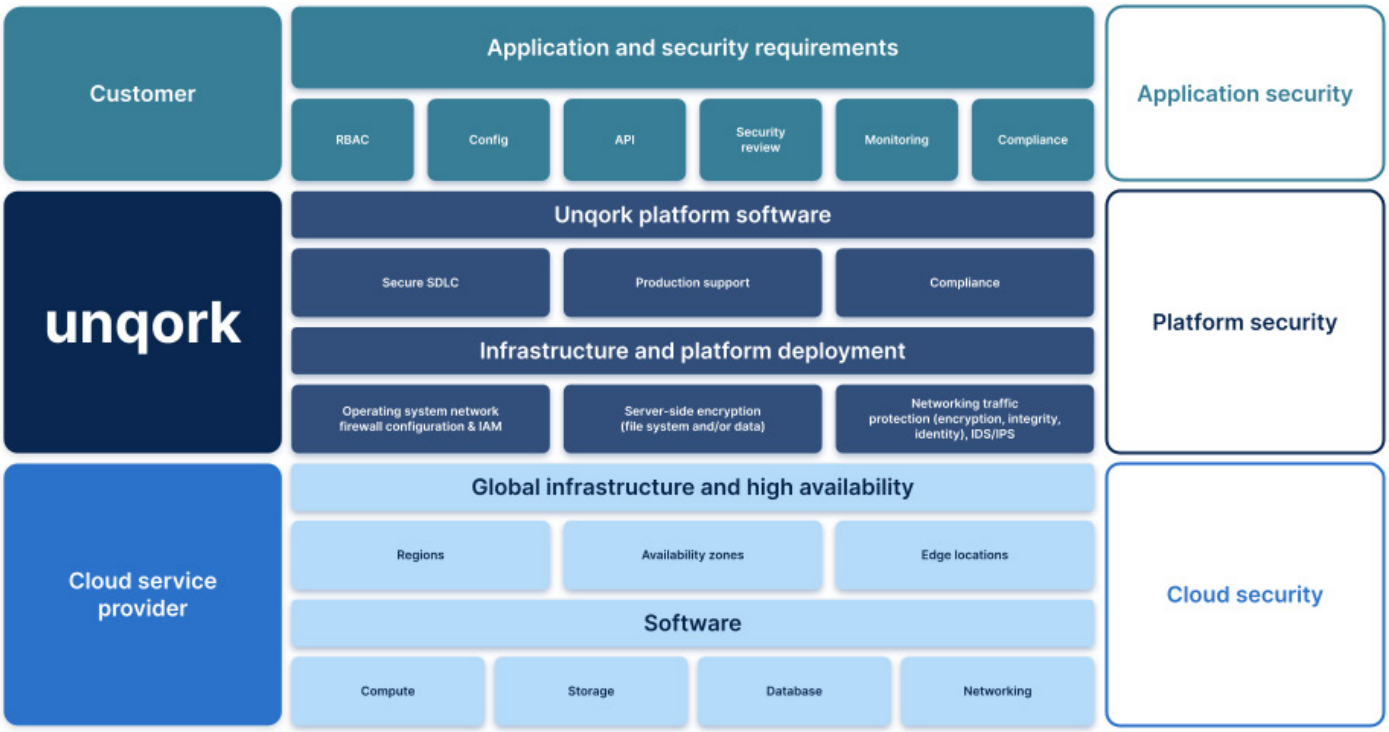
Shared Security Model

The core of Unqork's approach to security is in our **Shared Security Model**, which identifies the responsibilities owned and shared between **Unqork**, our **customers**, and our Cloud Service **Providers (CSPs)**.

Unqork provides the tools and guidance necessary to build secure applications on our platform. However, our customers are ultimately responsible for enabling these security features and creating security controls where required, while also considering applicable laws & regulations[1]. Unqork is responsible for securing the underlying platform that no-code applications are built on (i.e., server patch management, secure software development, and cloud security) and our CSPs are responsible for the physical security of the cloud infrastructure and ensuring high availability. With Unqork, you inherit layers of technology and applied security controls delivered by Unqork and its CSPs, which means you and your team can focus a greater share of your efforts on building and maintaining applications that add value to your organization.

[1]When you engage Unqork's Application Security Services, we provide hands-on expertise in configuring and delivering applications with manual and automated security testing in line with both business and compliance requirements.

The chart below depicts three critical layers of the Shared Security Model: **Cloud** (security responsibility falls to the CSP); **Platform** (Unqork); and **Application** (customer).



Application security

At the application layer, our customers are responsible for enumerating business and security requirements, and for leveraging Unqork configuration accordingly. Much like how Unqork's own security team reviews and evaluates the configuration of cloud infrastructure, customers are responsible for considering things such as their access model, API authentication mechanisms, and data schemes within Unqork.

Platform security

The Unqork platform is entirely managed by Unqork, meaning internal Unqork teams are responsible for the development, maintenance, and security of the Unqork platform itself. Focusing on security, this spans the full gambit of Unqork's internal development life cycle: From product grooming to code development, all the way to cloud monitoring. Our security program is aimed at delivering our platform with the highest levels of security possible, and leveraging a wide range of tools and risk-based security strategies to ensure that you can build enterprise-grade applications right away.

Cloud security

Unqork's chosen IaaS CSPs such as AWS or Azure are responsible for protecting the infrastructure that runs all of the services offered in a given CSP's Cloud. This includes controls such as physical access controls within their data centers, monitoring & management of underlying firmware, and personnel security such as background checks and general access controls.

Shared Responsibility Model

	Customer	Unqork	Cloud service provider
Password	Responsible for setting their own password policy in Unqork	Responsible for providing the means for customers to implement their own password policies, and for protecting passwords stored in the platform	No responsibilities
Authentication	Responsible for selecting their own authentication mechanism, and managing any associated requirements (e.g., certificates, licenses, etc.) Responsible for providing	the means for customers to integrate their own idp or authentication mechanism, and maintaining the integrity of these integrations (where applicable)	No responsibilities
Authorization	Responsible for enumerating appropriate roles, and establishing interpolarity with IdPs, where applicable	Responsible for providing the means for customers to set granular role-based access controls	No responsibilities
Security scanning	Perform regular scans and reviews of changes to their unique no-code solution	Responsible for scanning the underlying platform code, and the cloud infrastructure and network that supports it	No responsibilities
Encryption	No Responsibilities	Encrypting data in transit and at rest, and for associated key management operations	No responsibilities
Patch management	No Responsibilities	Performing patch management on underlying cloud infrastructure and supporting technologies	No responsibilities
Cloud security	No Responsibilities	Performing security scans, investigations, and threat detection on an ongoing basis	No responsibilities
Resiliency	No Responsibilities	Manage and deploy resilient cloud infrastructure.	No responsibilities
Hardware maintenance	No Responsibilities	No Responsibilities	Ensure the integrity and fidelity of the hardware underlying cloud resources managed by Unqork
Data center security	No Responsibilities	No Responsibilities	Enforcing physical access controls, and physical environmental controls (e.g. fire suppression, back up power supply)

More customer responsibility

Less customer responsibility

Enterprise Security

Security is rooted in everything that Unqork does. Our platform is designed with complex, highly regulated sectors in mind; your expectations for security, privacy, and compliance guide everything we do. Our teams' decades of collective security, technology, and industry-specific experience have informed the creation of a world-class, security-first SaaS.

Security incident response

Unqork's incident response & monitoring program centers on our Security Information and Event Management (SIEM) platform. Logs from the Unqork Platform, our CSPs, and other critical systems are sent to our SIEM, where they are evaluated by a combination of manual analysis, human-generated security policies, and anomaly-detection engines built with advanced machine learning.

To aid in the investigation of suspicious events, Unqork's security team leverages a combination of cloud and agent-based intrusion detection/prevention systems (IDS/IPS), as well as a cohort of native cloud tools such as web application firewalls (WAFs) and access analyzers.

In addition, the Security Team's incident response plan (IRP) has standardized policy and processes that include training and awareness, incident detection and reporting, containment, eradication, and post-mortem for continuous improvement. The IRP undergoes testing at least once a year, and our Security team works closely with Platform Operations during technology incidents to identify if/when a security nexus exists. Unqork provides 24/7/365 support with severity/priority remediation timeline offerings in line with your risk tolerance.

Security education & training

Unqork maintains a robust and continuous security training program. All employees are required to complete security awareness training, delivered by a senior member of the Security team, during their first week of employment. After that, employees complete monthly digital training covering a rotating list of topics relevant to Unqork's business and regulatory obligations. In addition, our Security team delivers annual security and privacy training to all employees, covering a wide range of topics such as new or emerging threats, security processes & procedures, and evolving data privacy laws. Lastly, Unqork provides role-specific security training to individuals with roles and/or responsibilities for specific domains (e.g., incident response, disaster recovery, engineering, etc.)

Vulnerability management

We offer a secure and robust platform that is continuously monitored for vulnerabilities and patched to meet the highest security. Continuous scanning includes daily static scans of the platform code and dependencies, weekly dynamic application security tests, and dynamic application security testing prior to your application go-live.

Penetration testing

Unqork regularly assesses its platform security with pentesting bi-annually (at least), including periodic independent network and application pentesting, in-house manual application review and testing, and client-driven application penetration tests.

Features & Controls

The Unqork platform provides a suite of features and controls that enable you to take a robust security- and compliance-minded approach to developing value-additive applications for your organization.

SDLC security, phase by phase:

Unqork makes it easy for organizations to manage and oversee the entirety of the Software Development Lifecycle (SDLC) in one central location, including the Plan, Design, Build, Test, Deploy, and Maintain phases. Unqork applies a security-first approach to each phase.

Plan
Regulatory, legal, and security requirements are considered when planning functionality changes to ensure the Unqork platform is able to meet your needs while adhering to all applicable laws and regulations.

Design
During the design phase, the proposed changes to the platform's critical architecture, authentication, authorization, and access control mechanisms are reviewed in-depth. This includes a Security Architecture Review at the application and module level, threat modeling, secure configuration review, and adherence to security best practices. This ensures the Unqork platform is architected securely.

Build
Unqork has built a robust build pipeline, which includes revisioning to track changes that are made to an application. The Modules Revision Dashboard provides a fully auditable history of application changes to track who made what changes and when they were made.

Test
Prior to promoting changes to production, the platform goes through a series of automated vulnerability assessments and manual penetration tests to ensure architectural and component level modifications don't expose the underlying platform to security weaknesses and critical vulnerabilities. Additionally, secure design requirements stated during the Security Architecture Review are validated against what was built.

Deploy
Once an application passes through QA, it's ready to meet the world—first through deployment into user-acceptance environments and then, when it's ready, into production. Unqork can help you efficiently organize and manage these crucial processes with in-app Release Management functionality. Unqork's Release Management Dashboard supports the deployment of applications by enabling Creators to create a release with one or more applications. This functionality is critical because Creators often promote multiple apps together, increasing productivity and reducing the risk of error.

Maintain

Because Unqork operates in an agile environment, a waterfall approach is cumbersome and not fit for purpose—making regular security maintenance critical. Similar to the Test phase, automated static code analysis (SAST) is conducted daily across the source code, security composition analysis (SCA) is also conducted to ensure libraries and dependencies are free from defects and mitigating controls are in place when discovered. Dynamic Application Security Testing (DAST) is regularly conducted leveraging an industry-leading application.

Additionally, weaknesses and vulnerabilities discovered throughout the SDLC process are tracked internally and prioritized for remediation and mitigation activities.

Data security & encryption

Unqork meets confidentiality, integrity, and availability requirements as well as the strictest information security and privacy standards. Unqork allows organizations to keep all data confidential, fully encrypted at rest and in transit, avoid unauthorized changes, and maintain redundancy for data and service availability.

All your data is securely stored within **MongoDB Atlas**, our cloud database services provider, ensuring AES256 encryption at rest. All communication and data in transit with and within the cloud network are also secured with TLS 1.2 HTTPS encryption.

Single-tenant architecture

All Unqork instances are single-tenant by default. Only your products, rules, and customers live inside of your instance. Every Unqork customer receives several non-production environments in a VPC separate from the production environment.

Networks & systems

Unqork uses a defense-in-depth methodology to mitigate any threats that might compromise the confidentiality, availability, or integrity of your data, assets, and services.

Our solutions feature edge-to-edge security capabilities that provide visibility, threat management, and remediation. To handle any security-related incidents, Unqork implements an incident management plan that includes continuous security monitoring and threat detection solutions including web application firewalls, network access control lists (ACLs), native and non-native cloud monitoring tools, and IDS/IPS.

Access management

The Unqork platform allows users to leverage granular RBAC capabilities to manage user access and permissions for each promotable item type and to create separation of duties across required roles.

APIs & integrations

One of the great benefits of Unqork is how it empowers organizations to seamlessly integrate custom applications with existing legacy systems and external third-party solutions. Whether it be an API, a custom integration, or a blue-chip technology partner, the Unqork platform allows users to authenticate these services through a multitude of methods while providing the means to apply TLS or other controls to further enhance integration security.

Secure system of record

WORM/system of record

Unqork eliminates the risk of original records being altered or deleted. You can write immutable information to a single disk one time and prevent editing, overwriting, renaming, or erasing while always maintaining the original submission.

Data lineage

Unqork ties submissions to the version of your application or form, with visibility of the data origin, what happens to it, and where it moves over time. See who has changed what, and when, with the ability to trace errors back to the root cause—drop any component into a form and create an audit trail of any interaction on a page.

Data versioning

Our platform makes it easy for you to archive individual data iterations, maintain persistent storage of your data, and record and store every submission change made from a record's creation until the present. You can create full snapshots in real-time and define how long your data is stored and when it will be purged.

Granular data retention/persistence

Collect all of your various data, including user session usage and session details. Review at your chosen granularity to visualize & evaluate concurrent data and manage the correlation of summary tables with raw data.

Certification & compliance

We understand that security is a primary concern for organizations that are evaluating cloud-based applications. Our SaaS operations conform to rigorous certification, compliance, and security programs and processes. We work with AICPA-certified third-party auditors to maintain security compliance with SOC 2 Type II and industry-mandated standards (e.g., HIPAA). SaaS services from Unqork comply with the following important certification and compliance standards:

SOC2 Type II

Unqork undergoes annual SOC 2 Type II examinations to attest to those security requirements. This examination is conducted in accordance with AICPA standards, specifically AT-C Section 205. On an annual basis, an external auditor evaluates the design of Unqork's security controls, to ensure suitable security assurance. Additionally, Unqork's controls are tested to verify control effectiveness.

GDPR
As per the definition of the General Data Protection Regulation (GDPR), Unqork processes client data as a Data Processor on behalf of its enterprise clients (the Data Controllers). Our organization and platform respond to—and allow our clients to comply with—privacy regulations such as the GDPR, and the California Consumer Privacy Act (CCPA).

HIPAA
Our team of experienced technology and healthcare industry specialists have designed our platform to manage all electronic protected health information (ePHI) in strict accordance with the Health Insurance Portability and Accountability Act of 1996 (HIPAA), so technology and healthcare companies are able to rapidly transform without sacrificing security. You can read more about our HIPAA compliance **here**.

FedRAMP
Unqork has initiated its journey to obtain FedRAMP authorization by Q1 2022. Key to this effort is Unqork's focus on using proven, authorized services and solutions including, but not limited to:

- All encryption internal and external uses FIPS validated cryptography suites
- Use of PIV/CAC authentication for US Government customers
- Implementation of DNSSec
- Zero-trust architecture

High Availability & Redundancy

When it comes to SaaS, reliability is a cornerstone. In relinquishing control of your software's backend infrastructure operations, you need a partner that you can trust to ensure the consistent availability and performance of your business-critical applications.

Unqork provides you with the reliability and availability to give you confidence that your employees and/or customers have access to your Unqork services, when they need it, and from where they need it.

Our always-on monitoring processes and technologies give you peace of mind knowing that your services are constantly being supervised and optimized.

We're committed to ensuring that your business-critical software is continuously up and running. SaaS solutions from Unqork operate at near-100% service availability levels[2] that we have a history of meeting and exceeding.

We deploy our SaaS solutions in a load-balanced and highly available infrastructure that's designed to handle heavy traffic and eliminate single points of failure at any level of the deployment architecture.

Failure detection capabilities exist within each tier, and once activated, send instant alerts to the Network & Security teams for correction. Additionally, failures are automatically contained, as redundant data backups allow single instances to fail without any impact on the service or user experience.

[2]A **recent analysis** found that Unqork boasted 99.99% uptime in 2020.

Automatic data & configuration backup

Periodic data backups are performed automatically and allow for one or more data recovery points, giving you the confidence that your data won't be lost.

SaaS solutions from Unqork come equipped with built-in data resilience, achieved by automated, scheduled backups of data and configurations that create multiple service recovery points. These are essential to business continuity and disaster recovery plans and, upon a customers' request, can also be utilized to restore service to a previous state.

Backup & restoration

Data backups are separately managed for each of our customers in order to meet the unique requirements of the client's policies and requirements. The following are some examples of backup and restoration procedures inherent in our SaaS offering:

Recurring backups
All data is routinely backed up and safely stored on a daily basis. Every six hours for transactional data.

Retention period
For most SaaS clients, data backup points are stored for a defined retention period of one calendar year. Clients may define any retention period they may require as short as 24 hours up to multi-year.

Storage policies
In case of disaster, additional backup snapshots are stored for use if a recovery effort is required.

Disaster recovery

Unqork's SaaS operations team manages the services necessary to restore your data as soon as possible following a disaster-type event. Our disaster recovery plan is regularly tested and updated to ensure optimal execution in restoring service should a natural or artificial disaster compromise your primary processing location.

The plan is based on two key metrics: recovery point objective (RPO) and recovery time objective (RTO). The RPO measures the maximum amount of recoverable pre-existing data, prior to the disaster, and the RTO measures the target restoration time of the service following a disaster.

Achieving these benchmarks is our main goal when facing a disaster recovery situation. Current Unqork RPOs are one hour and RTOs are four hours for each client resulting in best-in-class service.

In Conclusion

The pressures on organizations to "go digital" have never been greater. The Unqork platform takes on much of the "heavy lifting" of enterprise development, so companies can focus entirely on building value-generating applications. This is exactly why we have strived—and continue to strive—to develop a state-of-the-art security program embedded into all aspects of Unqork's platform. We want our customers to focus on innovation with the knowledge that they are using a platform where security has been a priority from day one.