



Enterprise Readiness

Last Updated: September 2022

Table of Contents

[Availability, Uptime, and Scalability](#)

[Tenancy](#)

[Availability](#)

[Monitoring system status](#)

[Disaster recovery](#)

[Release Process](#)

[Hotfixes](#)

[Early Access](#)

[Security](#)

[Data Encryption](#)

[Organizational Security](#)

[Vulnerability Assessments](#)

[Third Party Attestations](#)

Every year, tens of millions workers around the world find millions of jobs on Fountain's platform. We make significant investments in performance, reliability, release processes and security to ensure a frictionless experience for workers and for our enterprise customers. This white paper provides an overview of our platform and practices.

Availability, Uptime, and Scalability

Fountain helps job-seekers apply from around the globe using whatever device and internet connection is available, making system performance and availability critical concerns. Fountain has invested significantly over the past twelve months to expand our cloud infrastructure, tooling and expertise.

Tenancy

Fountain's platform is built on a multi-tenant architecture, enabling multiple customers to share and benefit from scalable infrastructure while logically isolating the application data

belonging to each customer. Fountain maintains multiple, isolated multi-tenant environments around the world for maximum performance and reliability.

Availability

Fountain's core platform achieves resilience and elasticity through technical features including:

- horizontally scalable, stateless compute infrastructure
- local content-delivery network (CDN) nodes for static assets and application resources
- isolated availability zones within each global region
- fault-tolerant (primary-replica) storage infrastructure with routine backups
- active monitoring and failover of compute resources

Together, these features enable high availability and maintain a standard Service Level Agreement (SLA) of 99.99% uptime for critical systems.

Monitoring system status

The current status and recent uptime of Fountain's core platform and critical 3rd-party providers are available from status.fountain.com.

Disaster recovery

Fountain maintains Business Continuity and Disaster Recovery (BCDR) plans to ensure the system can recover from various catastrophic (if improbable) scenarios. These scenarios range from regional utility outages to Distributed Denial of Service (DDoS) attacks against critical infrastructure. These plans are tested through regularly-scheduled simulations that assess both internal readiness and compliance with our platform SLA.

In addition to the high-level SLA, Fountain evaluates performance in Disaster Recovery simulations against three key targets:

- Maximum Tolerable Downtime (MTD). The MTD represents the total amount of time Fountain leaders/managers are willing to accept for a mission/business process outage or disruption and includes all impact considerations. The MTD for Fountain's platform is 1 hour.

- **Recovery Time Objective (RTO).** RTO defines the maximum amount of time that a system resource can remain unavailable before there is an unacceptable impact on other system resources, supported mission/business processes, and the MTD. The RTO for Fountain's platform is 1 hour.
- **Recovery Point Objective (RPO).** The RPO represents the point in time, prior to a disruption or system outage, to which mission/business process data must be recovered (given the most recent backup copy of the data) after an outage. The RPO for Fountain's platform is 15m.

Release Process

Fountain releases new code to our production systems up to multiple times per day. Our production release process is highly automated and leverages multiple test suites and production monitoring to ensure high quality.

During our normal developer workflow, all code is subject to our full developer test suites, from unit tests up to end-to-end browser tests. New features and bug fixes go through a pull request and code review cycle, then another full test suite run. If this test suite passes, we merge the code into our master branch.

When making a release, our Release Engineering (RelEng) team cuts a release branch that gathers all changes and runs the test suites again. When all tests pass, the team ships this code branch to Production systems. Release notes are published at least weekly to new.fountain.com, summarizing all important changes.

Hotfixes

When an issue is found in Production that prevents our customers from hiring new applicants, or another Severity 1 problem occurs, we employ a hotfix process to take immediate action. This involves making the smallest possible change to the version of code that is on Production, running a set of test suites, and when they pass, deploying the fix. This accelerated process allows us to fix critical bugs in hours or minutes.

Early Access

All new work is deployed to all Production systems concurrently. However, new features that are not yet complete or designated as Early Access are gated behind feature flags that can be enabled or disabled on a per-customer basis. As Early Access features develop, they are gradually rolled out to more customers (typically via an opt-in process). We actively collect feedback and iterate before rolling out Early Access features to all customers.

Security

At Fountain, the safety and security of customer data and personal information are a top priority. We built the Fountain platform with global security standards in mind, with a commitment to maintaining high data privacy and security standards through continuous investments in our systems, processes, and culture.

Here are some of the key security measures that we take to keep your data secure:

Data Encryption

Fountain uses enterprise-grade encryption for secure communication and storage of application data. We use TLS 1.2 or higher encryption standards to protect customer data and personal information in transit. At the backend, we encrypt customer data at-rest using industry-standard encryption algorithms and techniques.

Organizational Security

At Fountain, security is a shared responsibility. We provide all employees with security and privacy training as part of their onboarding, and at a regular cadence to safeguard both Fountain and our customers' data.

We also require all our employees to use strong and unique passwords and to set up two-factor authentication where available.

Vulnerability Assessments

Fountain uses automated security tools to continuously scan for vulnerabilities and ensure that they are addressed.

Additionally, Fountain engages leading third-party security firms to conduct security reviews and penetration testing to identify potential vulnerabilities and ensure that they are remediated.

Fountain Penetration Testing report is available upon request. Please reach out to your Account Executive for details.

Third Party Attestations

Fountain engages third-party auditors to conduct independent verification of our security and compliance controls. Fountain is currently audited against the following international standards:



Fountain undergoes rigorous independent third-party SOC 2 audits conducted by reputable AICPA certified firms. The audits evaluate the effectiveness, efficiency, and appropriateness of security and compliance controls within a specific period. Please reach out to your Account Executive for details.

Fountain's SOC2 Type 2 report is available upon request. Please reach out to your Account Executive for details.