fountain

Security & Privacy Infrastructure

How Fountain Protects Applicant and Employer Data with Industry-Leading Security Practices

July 2025

Introduction

At Fountain, we consider security to be one of our most important missions. Our customers and their applicants entrust us with their data when applying for positions, add a new worker to be onboarded, or create a new Shift. We work tirelessly to implement controls and procedures to keep this data safe. We prioritize security in everything we do, and this paper outlines our approach to achieving it. Our approach includes industry-leading regulatory compliance, strong security controls, a culture of security within Fountain, and a highly available and scalable architecture. This paper provides an overview of our security approach in each of these areas.

Certifications & Regulatory Compliance

Fountain is excited to announce that it has achieved ISO 27001 certification, one of the most globally recognized information security standards, in addition to our SOC-2 Type 2 compliance. Each certification is a significant milestone in Fountain's journey to establishing itself as a leading provider of enterprise software solutions, it demonstrates Fountain's commitment to keeping its customers and stakeholders data safe and secure. Additional details are available at trust.fountain.com

Service Organization Control 2

SOC 2 is a type of audit and report that measures how well a service organization meets a set of standards established by the American Institute of Certified Public Accountants (AICPA) for evaluating the controls of service. The SOC 2 audit process involves an independent auditor examining Fountain's controls and providing a report that details the organization's compliance. We have the trust principles in Security, Confidentiality, and Availability.

ISO 27001

Fountain is committed to building customer trust, Receiving third-party attestations like SOC-2 Type 2 and ISO 27001 demonstrates to customers and prospects the maturity of Fountain's information security program. The ISO 27001 is one of the gold standards in security certifications.

GDPR

Complying with GDPR is a paramount commitment that Fountain makes to our customers, ensuring their privacy and data protection are upheld with the highest standards. By adhering to GDPR regulations, Fountain demonstrates its respect for individuals' personal information, fostering a sense of trust and transparency. Customers can rest assured that their data is handled responsibly, safeguarding them from potential breaches and unauthorized use.

SOC 2 Type II

ISO 27001:2022

GDPR

CCPA

SOC 1 Type II

Security Controls

Fountain maintains strong security controls in our product and our product's platform that are in line with industry standard security best practices. We regularly assess ourselves against these standards internally and with third-party vendors and audits.

Security Tooling and Monitoring

We use industry leading security tooling to detect threats at the endpoint, network, and cloud level. Our robust alerting on these tools are monitored 24/7.

We log and monitor various system aspects such as application, infrastructure, network and storage events, performance and utilization. Event data is securely aggregated, masked, and stored to prevent tampering, in compliance with Fountain's data retention policy.

Network Segmentation

Fountain follows industry best practices to design and segment our network between different operating domains. Our production and non-production environments are completely isolated from each other to prevent any data flow from a production environment to our non-production environments. It also provides additional benefits where any availability or security impact of a non-production environment doesn't have any effect on the production environment.
We also operate in various regions and each region is segmented from all other regions with only network traffic permitted as necessary, keeping in line with local regulations.

Encryption at Rest

Encrypting all data, everywhere is a fundamental part of our security strategy. We use industry standard encryption algorithms such as AES-256 to encrypt our data everywhere it's being stored. This ensures that unauthorized actors cannot access or manipulate the data stored in our systems.

Encryption in Transit

In addition to protecting our data at rest, we are also committed to protecting our data in every part of its transmission. We encrypt data in transit using industry standard protocols like TLS that prevent eavesdropping, intercepting, or modification of this data.

Data Security

At Fountain, safeguarding customer data, applicant data and employee data, including any Personal Identifiable Information (PII) of is our top priority.

We have strict policies, processes and technical safeguards that prevent usage of any production data in non-production environments. Instead, we generate test data for all of our staging and development environments and also for any training purposes.

Fountain's data retention policy ensures that data is not kept longer than necessary and our encryption policy ensures data is always encrypted at every stage of its lifecycle.

Authentication and Authorization

Single Sign On (SSO)

SSO is a critical component of our internal security strategy. We make use of SSO whenever possible to streamline the login process for our user and minimize the need to use long-term credentials or shared credentials.

Fountain also supports Single Sign On for your users to access Fountain. We support the SAML 2.0 standard with "Just In Time" provisioning for your users. This allows you to use an authentication solution that your users are already familiar with, without the need to create a new login for Fountain. This option makes it very easy to onboard new users, offboard old users, use existing multi factor authentication methods, and have regular rotation of their passwords.

Multi Factor Authentication

We leverage industry best practices in the multi-factor authentication (MFA) space by using a variety of methods like one-time passwords, biometrics, and hardware tokens depending on the sensitivity and criticality of the application being accessed.

Role Based Access Control

Role Based Access Control, known as RBAC, allows us to define and enforce granular access permissions based on a user's role and responsibilities. The Fountain application allows you to assign a user to one of our built in roles or create a new role based on the access a user needs.

The roles for our internal applications are regularly reviewed and updated to ensure an appropriate separation of duties, alignment with industry best practices, and adherence to the principle of least privilege. For internal applications that support the feature, we've implemented step-up authentication to require users to provide an additional factor of authentication when accessing sensitive resources or performing production altering changes.

Key Management and Rotation

Our Key Management System ensures the highest level of data protection by controlling access to encryption keys, preventing accidental deletion of encryption keys, and regularly rotating encryption keys in line with industry best practices. This system is seamlessly integrated with our platform, designed to be transparent to our users and developers.

Application Security

Fountain has a vulnerability management program to continuously monitor for vulnerabilities that are discovered internally through vulnerability scans and from employees. We also encourage external vendors or researchers to report security issues to us through our security reporting program available at fountain.com/security

Fountain prioritizes the resolution of vulnerabilities according to their risk, as determined by the likelihood and impact ratings.

AI Security

AI is at the core of Fountain's latest platform offerings as Fountain helps customers to automate tasks across the Frontline hiring journey. Fountain takes a strong security first approach in this new domain including monitoring, guardrails and safety controls, and strong internal guidelines around AI usage internally at Fountain.

Comprehensive Monitoring

Fountain has implemented robust monitoring capabilities across our AI usage to ensure a high level of accountability. Every agentic action that the platform takes is logged, traceable, and explainable. Fountain captures a complete audit trail of all AI actions including inputs, outputs, and request metadata. This monitoring allows Fountain to continuously improve system performance and monitor AI usage and spend.

Guardrails and Safety Controls

Fountain has implemented robust guardrails and safety controls to protect the system and our end users. Fountain has a moderation layer for our AI usage to detect harmful and inappropriate content and identify potential concerns like prompt injection or possible hallucination.

Internal AI Usage Policy

Fountain has established a comprehensive internal AI usage policy that guides employees on their interaction and implementation with AI tools. The policy helps ensure that AI is used in a way that is safe and protects Fountain's proprietary data. Fountain has established an AI Board that helps oversee the governance of AI at Fountain and implement industry leading safety controls.

Web Protections

To maintain the availability, security, and integrity of our platform, we have protections in place to minimize the impact that malicious actors, like “bad bots”, can have on our website, we partner with industry leading bot management, web application firewall, and rate limiting solutions to filter out this activity. We process

Bot Mitigation

Fountain offers a Bot Mitigation feature that can detect and block malicious bot activity from submitting applications to all Fountain hosted application forms. This helps ensure a high quality of applicant submissions and high availability of our application site. All visitors to our site are scored on the likelihood of being a bot and then are blocked if they try to submit an application. As you may know, not all bots are bad, and our rules still allow good bots to permit services like search engine optimization so applicants can quickly and easily find your job posting.

Our web protection features are capable of handling a high volume of malicious requests, including a peak upwards of 100,000 requests per hour during a bot attack. We typically successfully deflect upwards of 2.5 million malicious requests per month.

Web Application Firewall

In addition to Bot Mitigations, we also partner with an industry standard Web Application Firewall (WAF) provider to block malicious traffic. A WAF or web application firewall helps protect Fountain’s applications by filtering and monitoring traffic between a web application and the Internet. It protects our web applications from attacks such as cross-site forgery, cross-site-scripting (XSS), file inclusion, and SQL injection, among others. This feature is part of a suite of tools which together create a holistic defense against a range of attack vectors keeping applicant data secure.

Advanced Rate Limiting

To help further mitigate spam applicants, we can supplement our existing protections with Advanced Rate Limiting rules in place that allow us to limit the volume of applications based on a number of factors like IP Address, User Agent, Source ASN, and other custom logic based on our analysis that we’ve tuned over the years using the millions of requests we observe daily. These rules allow us to protect our customers from a high volume of fraudulent applications.

Security Culture

At Fountain, building a security culture is essential to ensuring the protection of customer, applicant and employee information. We strive to instill a sense of responsibility for security among all employees and promote a culture of proactive risk management. This is achieved through regular training and education, establishing clear policies and procedures, and encouraging open communication and reporting of security incidents. By promoting a security-focused mindset, we protect ourselves against potential threats and ensure the long-term security and success of our operations.

Auditing and Penetration Testing

We undergo continual internal auditing against industry standard security controls to ensure that we are always in a compliant state. We also undergo annual auditing from an independent third party against industry standard compliance frameworks like SOC2 and ISO 27001.

Fountain undergoes annual security penetration tests conducted by an external vendor to detect network and application security vulnerabilities. The findings from these tests are evaluated, documented and assigned to the appropriate teams for remediation based on risk.

Internal Security Team

We have an internal security team of Governance, Risk and Compliance engineers, Security Engineers, and a Data Privacy team that work around the clock to detect threats against Fountain and minimize risk.

Background Checks

Fountain performs background verification checks on potential personnel who will have access to confidential information, such as Customer Data and Applicant Data, in accordance with applicable laws and regulations. The scope of the background checks is based on the job duties of the individual.

Onboarding

New employees are required to sign confidentiality agreements and comply with our Acceptable Use Policy during the onboarding process.

Employees participate in a security onboarding session on their first day that informs them of security policies and procedures and we ensure that their new accounts are created and protected with security best practices.

Employee Reporting

We encourage employees to report issues they find in Fountain so that we can address them, this includes security issues. We also offer an anonymous reporting line for employees where employees can report security concerns.

Security Training

We require our employees to participate in our annual security awareness training.

We also run frequent phishing campaigns to ensure security is top-of-mind for our employees and informs and educates them on the latest security threats.

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 made significant investments to expand our cloud infrastructure, tooling and expertise.

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 application resources
- isolated availability zones within each global region
- fault-tolerant (primary-replica) storage infrastructure with backups
- active monitoring and failover

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

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).

Scheduled Maintenance

Fountain's platform is designed to maximize availability and uptime, but scheduled maintenance windows are occasionally required to upgrade and extend our services. Our policy is to provide a minimum of two weeks' notice ahead of any maintenance window and schedule our work to minimize the impact on production services and business processes.

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.

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.

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.

Fountain conducts quarterly live drills to assess the processes, playbooks, and employee training needed to recover from various simulated disaster scenarios. These drills include:

- Testing team / human-factors response to a simulated disaster
- Live recovery of critical infrastructure and systems in the wake of the simulated disaster (e.g. live failover from a production region to a DR region)
- Verifying data replication and backup processes
- Verifying system integrity post-recovery
- Verifying compliance with documented SLAs
- Conducting a full post-mortem on the DR exercise
- Revising DR playbooks in response to the drill and post-mortem

Scalability

We operate highly scalable infrastructure designed to scale up or down as our application needs change. Our usage of Content Delivery Networks (CDN), load balancing, and intelligent routing ensure that our site is always available and quick to serve our customers and their applicants.

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.