Security and Reliability Overview

gain

Introduction

We work hard to ensure Gain is a safe platform for its users. We understand that businesses rely on us to protect their data, security, and reputation of their brands and their own customers, and we take that responsibility seriously. The following is an overview of our security standards, practices, and policies.

Infrastructure

Main application platform. Gain's main infrastructure is hosted on Heroku, a trusted, renowned cloud application platform from Salesforce that manages all aspects of security at every layer from physical to application. Heroku's physical infrastructure is, in turn, completely hosted and managed within Amazon's secure data centers using Amazon Web Services (AWS) technology. Gain also uses AWS services directly.

Amazon data centers are ISO 27001 and FISMA certified, with multiple layers of physical protection. Physical and data access is strictly controlled to both staff and visitors, provided only when legitimately needed, and is logged and audited constantly. Environmental safeguards include comprehensive fire and power/electrical protection, and climate/temperature control.

The cloud application platform manages all network firewalls in a secure manner, and provides automatic DDoS mitigation, spoofing/sniffing protections, and automatically blocks port scanning attempts.

Gain runs within its own isolated environment in the cloud application platform and cannot interact with other applications or areas of the system. This restrictive operating environment is designed to prevent security and stability issues. These self-contained environments isolate processes, memory, and the file system using LXC while host-based firewalls restrict applications from establishing local network connections.

For more information about Heroku security, privacy and certifications, visit https://www.heroku.com/policy/security and https://devcenter.heroku.com/articles/security-privacy-compliance. For more information about Amazon AWS security, visit https://aws.amazon.com/security.

Third-party providers. Gain uses other third-party providers for various specific aspects or features of the product (examples: video transcoding, image processing). These providers are either hosted on AWS themselves or sit on infrastructure that is held to the same standards as our main infrastructure.

Data

Data location. All of Gain's data is stored and processed in the United States. For speed purposes, some data may be cached temporarily in a Content Delivery Network (CDN) with nodes distributed in various parts of the world.

Encryption in transit. All data processed by Gain is encrypted in transit using SSL everywhere. This includes all communication between Gain servers and end user devices, server-to-database, and server-to-server communications.

Encryption at rest. Our databases are encrypted at rest with AES-256, block-level storage encryption. Uploaded videos, files, and images are protected in non-browsable Amazon S3 storage with non-discoverable key names (uuid-based) that can be shared only by a user with knowledge of the full url. Passwords are stored using the PBKDF2 algorithm with a SHA256 hash, individual, random salting and multiple hashing iterations (tens of thousands).

Backups and durability. Every database change is written to write-ahead logs, which are shipped to multi-datacenter, high-durability storage. In the unlikely event of unrecoverable hardware failure, logs can be automatically replayed to recover the database to within seconds of its last known state. This continuous backup allows Gain to roll back a database to any specific point in time within the last 7 days. Additionally full backups are automatically performed every day. Daily backups are retained for 7 days, weekly backups for 8 weeks, and monthly backups for 12 months. Gain performs data recovery drills regularly.

Customer data deletion. Gain retains customer data by default upon cancellation, in case the customer decides to reactivate their account, but customers can request their data to be completely deleted from our systems at any time. These data protection rights must be extended to members of the European Union / European Economic Area, in accordance with the GDPR. However, in an effort to provide broad data protection to our customers, we extend these rights to all users of the service. To read about these and other personal data rights in detail please visit our Privacy Policy page.

Billing data. Gain uses Stripe for all billing and payment functions. Stripe is audited by a PCI-certified auditor and is certified to PCI Service Provider Level 1, the most stringent level of certification available in the payments industry. Gain follows all of Stripe's recommended integration methods, thus no sensitive credit card data is ever seen or stored by Gain servers. Gain submits a PCI compliance self assessment (SAQ 3.2.1) every year. We can provide this PCI compliance certificate upon request.

Law enforcement. Gain does not hand over data to law enforcement unless (i) there is applicable law, court order, or regulation that compels us, (ii) to exercise, establish or defend our legal rights, or (iii) to protect your vital interests or those of any other person. To date, Gain has never received an order for customer data from a law enforcement organization. To read our full policy on information disclosure, please visit our Privacy Policy page.

Application

Development practices. Gain follows web security best practices and is constantly being tested against the latest vulnerabilities and attacks outlined in the OWASP Top Ten and others. All components of the application stack are constantly kept up to date with latest security updates.

Penetration testing. Gain maintains a bug bounty program through HackerOne where security researchers are regularly invited to perform penetration tests. Public researchers are welcome to report found vulnerabilities and often do. As of this date, Gain has awarded over $1000 in bounties to researchers in the last four years for their responsible bug disclosures.

Access to Social Networks. Connections to social networks (Facebook, Twitter, Instagram, LinkedIn, etc.) are done using each network's official authentication API and best practices. These connections are done using Oauth2 or variants of it, which means Gain never sees a social account's password. Instead, Gain receives a time-limited access token which end users can revoke at any time. All communication to these external APIs is done exclusively through SSL. We will never use social APIs in ways that violate the networks' terms of service. This is crucial to ensure we are always in good standing with our partners.

End user security. All user passwords are stored using the PBKDF2 algorithm with a SHA256 hash, individual, random salting and multiple hashing iterations (tens of thousands). For extra security, users are alerted via email whenever their password is changed. Gain also offers a "passwordless login" option for content reviewers that allows them to log in with a secure, short-lived, on-time-use token sent in an email message. All users can choose to enable two-factor authentication to provide an extra layer of protection to their accounts.

Monitoring and logging. Gain stores comprehensive event and access logs on its servers, and monitors them for irregular activity or intrusion attempts. Our cloud application platform provides DDoS mitigation and protection against intrusions at the network level.

Scaling and Reliability

The Gain platform has been built and perfected through careful design, solid architecture principles, and over 6 years of real-world experience. We've battle-tested Gain to make sure it is performant and reliable.

User experience. The Gain app itself is a modern web application that is constantly scaled horizontally as user base and traffic grows, and is constantly monitored for performance under heavy loads. This means that clients can expect a responsive, enjoyable experience every time they use the app, without hiccups or errors.

Volume. The Gain scheduling engine is built on a constantly tested, reliable system that can handle the publication of thousands of Facebook, Twitter, Instagram, and LinkedIn posts at once. As of this writing, Gain has successfully published over 3 million posts to social media networks, and currently handles over 100,000 posts per month. We currently serve customers with thousands of users under a single account, and some of these larger accounts handle over 6,000 posts per month.

Content pre-check system. Through an automated pre-check system, every post is pre-checked for compliance with each social network's specs and post requirements to minimize any chance of error before it is even published.

Fail-safe publishing. Our system handles publishing of scheduled posts through an array of parallel worker servers that ensure multiple posts from multiple customers can be published at the same time without delay.

If any error occurs during the publishing process for any reason, the error is immediately logged in the post's history, visible to the end user, and designated users in the customer's organization are notified through email and/or browser notifications, as well as the Gain UI itself. These notifications provide a link that will take you directly to the content that failed to publish so you can take action right away (reschedule the post, push the post live, etc.)

Even then, Gain will automatically retry a failed post up to three times within a ten-minute period. This usually takes care of certain types of transient errors, such as the social network itself having platform issues.

A step further: Facebook native publishing. For Facebook posts, customers can choose to use either Gain's internal scheduling engine or Facebook's native scheduling engine. When Facebook's engine is selected, posts are always sent to be scheduled on Facebook's side, rather than Gain's side. This adds an extra layer of certainty that content will be published at the right time because Facebook's native platform is handling the task. Even if you need to edit a post that's already been scheduled on Facebook, you can do so on Gain and those changes will be reflected on Facebook's native scheduling platform.

Another reason Gain relies on Facebook to schedule the posts is to allow teams to create multimedia campaigns or prepare promoted posts before the content is published. This can only be done when the post has been scheduled on Facebook for a future publishing date.

Finally, Gain has another layer in the Facebook scheduling system that monitors all of the content scheduled to the social network to ensure that Facebook is indeed publishing posts at the correct time. So even if Facebook fails to publish a post, we provide a fallback and will automatically retry to publish the post from the Gain side.

Personnel and Access Control

Personnel. All employees and contractors sign confidentiality agreements before gaining access to Gain code and data. Background checks are not performed. All personnel is trained regularly about security best practices for Gain systems and their own equipment.

System access. Access to core Gain systems or any system where customer data is kept is provided to employees on a ”need to know” and “least privilege” basis. All employees are provided with a centralized, enterprise-grade password management system. Password sharing is prohibited except in rare instances where a non-critical third-party system does not provide multiple account functionality. Two-factor authentication is enabled and enforced on all third-party systems that support this option. Upon termination of employment, access to all systems is thoroughly reviewed and revoked immediately.

Incident Management

Procedures. We have procedures for responding to security incidents. Upon the discovery of a security breach customers will be alerted immediately and we will continue providing constant public updates regarding the impact of the incident and mitigation measures taken. We will also contact account owners directly and be available directly to answer questions. After the incident is resolved customers will be provided with a full report including a description of the root cause and steps taken to ensure the situation is fixed looking forward. To date, Gain has never had any major security incidents.

Want to Know More?

You can contact us at any time if you have any other security-related questions. We're glad to talk to you.

www.gainapp.com