handwriting.io

Technical Security Policy - June 13, 2016

Overview

Handwriting.io is a patented API that enables the use of authentic digital handwriting across print and digital media in a scalable and affordable way. We help businesses increase sales, enhance brand identity and communicate more effectively with customers, investors, employees, and the media. By putting customers at the center of communications, we help businesses use personal messages to achieve at least 10x engagement response rates.

Handwriting.io's state of the art technology is backed by a highly reliable infrastructure built in the cloud. We have fully redundant systems, as well as security policies and procedures, failure procedures, and data retention policies to ensure any component failure will not cause a loss of accessibility to our products.

The company was founded by Eloise Bune and is headquartered in New York, NY. Learn more at handwriting.io.

Physical Security

Our physical infrastructure is hosted and managed by Amazon Web Services (AWS), which manages ISO 27001 certified data centers. AWS data centers are housed in nondescript facilities. Physical access is strictly controlled both at the perimeter and at building ingress points by professional security staff utilizing video surveillance, intrusion detection systems, and other electronic means. All physical access to data centers by AWS employees is logged and audited routinely.

Certifications

Amazon's data center operations have been accredited/certified under:

- SOC1 / SSAE16 / ISAE3402 (formerly SAS70)
- SOC2
- SOC3
- FISMA
- PCI DSS Level 1
- ISO9001 /ISO27001 / ISO 27017 / ISO 27018

Fire Detection and Suppression

Automatic fire detection and suppression equipment has been installed to reduce risk. The fire detection system utilizes smoke detection sensors in all data center environments, mechanical and electrical infrastructure spaces, chiller rooms and generator equipment rooms. These areas are protected by either wet-pipe, double interlocked pre-action, or gaseous sprinkler systems.

Power

The data center electrical power systems are designed to be fully redundant and maintainable without impact to operations, 24 hours a day, and seven days a week. Uninterruptible Power Supply (UPS) units provide back-up power in the event of an electrical failure for critical and essential loads in the facility. Data centers use generators to provide back-up power for the entire facility.

Climate and Temperature

Climate control is required to maintain a constant operating temperature for servers and other hardware, which prevents overheating and reduces the possibility of service outages. Data centers are conditioned to maintain atmospheric conditions at optimal levels. Personnel and systems monitor and control temperature and humidity at appropriate levels.

Management

AWS monitors electrical, mechanical, and life support systems and equipment so that any issues are immediately identified. Preventative maintenance is performed to maintain the continued operability of equipment.

Storage Device Decommissioning

When a storage device has reached the end of its useful life, a decommissioning process is used that is designed to prevent customer data from being exposed to unauthorized individuals. AWS uses techniques detailed NIST 800-88.

Fault Tolerance & High Availability

AWS has designed its systems to tolerate system or hardware failures with minimal customer impact. Data centers are built in clusters in various global regions. Our infrastructure is

architected in a way to take advantage of multiple regions and multiple availability zones within each region.

Network Security

Port Scans

Unauthorized port scans are strictly forbidden and are considered a violation of our infrastructure provider's Acceptable Use Policy. When an unauthorized port scan is detected, it is stopped and blocked. Port scans are ineffective as we restrict all non-HTTPS inbound ports.

IP Spoofing and Packet Sniffing

Our host-based firewall infrastructure will not permit a server to send traffic with a source IP or MAC address other than its own. Packet sniffing is prevented by our infrastructure including the hypervisor, which will not deliver traffic to an interface to which it is not addressed.

Access

Access to systems is restricted by individual access keys, public-key cryptography, and Access Control Lists (ACL). This provides us with an advanced level of security by limiting external access using multiple forms of control.

Data Security

Data Transmission

All data exchanged with our systems is sent over secure (TLS) connections. We strictly enforce HTTPS for all communications. We maintain SSL certificates on all external-facing systems and update our certificates on a regular basis. Using a secure TLS connection ensures that the data sent between our systems and you are authentic and encrypted while in transit. All data that is transmitted between our API servers and any backends systems, such as database servers, is also transmitted over a secure TLS connection.

We utilize Layer-4 load balancers to direct communication between frontend and backend servers and protect our backend server from external threats. This provides us with an extra

layer of defense against potential attacks and allows us to maintain a fault tolerant and resilient infrastructure.

Open Ports

Our systems are protected by a complete firewall solution. Inbound traffic is blocked on all ports to all backend servers with the exception of port 443, which is required for accessing our API.

Rate Limiting

We monitor logins and restrict access when malicious attempts are made. We track the number of calls made based on API token and IP address and restrict access if thresholds are exceeded. This is to ensure our system is never overloaded by a malicious or rogue user.

Data Encryption

We record each and every HTTP call within our auditlog. It is stored in a time-series database separate from our front-end database servers. We store your Account ID, API token key, general information about the HTTP request (ie: user agent, remote address, status code, duration, etc), and an encrypted copy of the text you rendered. This is the text you or your system has supplied us to generate an image using our patented handwriting technology. Our auditlog is the only place your text is stored. It is filtered out of all our logging and alerting systems. We encrypt the text at rest using the AES-256 encryption algorithm.

This information is stored to protect ourselves and our product. We primarily use this data for billing purposes and to protect ourselves against billing and usage disagreements. Storing this data also means we can ensure you are being billed accurately and fairly.

The encrypted text we store is only decrypted in the event of a billing dispute where we need to provide verification of your usage. If this does occur, only data from the account in question will be analyzed. No other accounts' data will be decrypted.

Data Retention

All raw data stored in our auditlog is retained for 90 days. Backups are retained for 90 days as well and we continue to store analytical data for 3 years. This analytical data does not include your encrypted render text. All databases containing system and customer data are fully redundant within two or more zones as well as fully backed up on a daily basis.

System-Level Security

System Access

System access is limited to Handwriting.io Operations and Development team members and requires public-key authentication using ssh keys. Additionally, systems running within our infrastructure do not allow password authentication to prevent password brute force attacks, theft, and sharing.

Application Security

We deploy to our infrastructure servers by leveraging continuous testing and integration tools. No system is put into production if it cannot pass our tests. We practice continuous deployment with no downtime. We've built our systems to be able to deploy updates, bug fixes, and features without any planned downtime.

We utilize an army of third-party services to keep us up to date with what's happening on all our systems. We have a 24/7/365 incident response team that is ready in the event of a serious failure. We continuously monitor our system's scalability, security, and availability.

The servers our applications run on are replaced on a weekly basis or on-the-fly when necessary and are replaced with the latest updates and security fixes with zero interruption of service.

We run load tests on production code on a scheduled basis to ensure changes we make do not negatively impact our performance and our handwriting technology continues to provide speeds that allow our customers to scale our technology.

Source Code

The source code for our API and handwriting technology is stored within a secure 3rd-party tool. We take daily backups of our source code and store it securely in two or more regions.

Vulnerability Scans and Best Practices

At Handwriting.io, we run weekly vulnerability scans against our website to ensure we are protected against serious threats, including the OWASP Top 10 Most Critical Web Application

Security Risks, which has become the industry standard for categorizing the most critical risks faced by web applications. All vulnerabilities are evaluated and reviewed to determine if it is applicable to our environment and are resolved based on the vulnerability severity.

We use modern web frameworks and the follow best practices of these frameworks. We are continuously updating our code and apply patches and updates to our servers on a regular basis.

Environments

We maintain separate. segregated Production, Staging, QA, and development environments. Production data is never stored in development environments.

Authentication

API Authentication

To use the API, customers will need an access token pair. All active accounts have the ability to create an unlimited number of access tokens and each access token is linked to the specific account that created it. No two access token pairs are alike.

Your token pair (key and secret) are randomly generated strings created by our system and should be included in all requests as the “username” and “password”, passed using HTTP basic access authentication.

Customers have the ability to create two types of tokens, Test tokens and Live tokens. Test tokens generates watermarked images and will not count against your plan usage. Live tokens generates un-watermarked images and will count against your plan usage. If you are subscribed to a paid or enterprise plan, you will be able to generate both Test and Live token types. Test tokens are ideal for situations such as development stages, proof of concepts, and QA testing. Live tokens are ideal for production-ready, user-facing applications.

Website Authentication

We utilize a 3rd-party tool to handle authentication to our website (handwriting.io). We never store your password within our systems. As an alternative to password authentication, we provide the option to use our website via multiple OAuth providers (such as Github or Google,

for example). OAuth provides a method for users to grant us access to a customer's resources without sharing their passwords. For more information, contact us.

Billing

Payment Information Storage

When payment information is provided to us, it is encrypted and transferred securely over HTTPS to our billing service provider, Chargify, who stores your payment information with our payment service provider, Stripe. We never store your payment information on our servers.

Both Stripe and Chargify are Level 1 PCI Compliant, which is the highest level of certification provided by the Payment Card Industry Security Standards Council.

Usage Reporting

Subscriptions are generally billing on a monthly or annual basis, but customers may be billed differently depending on the subscription agreement terms. Subscriptions that are billed based on usage will be billed as follows:

- Usage can be defined as, but not limited to, number of characters or number of images.
- We only calculate usage that was created by a "Live" (un-watermarked) token and update your usage on an hourly basis.
- Usage is calculated by account and includes usage for all API tokens owned by the account.

Disaster Recovery

Handwriting.io maintains redundancy within each component of our application to prevent single points of failure. We utilizes multiple zones for all system components and replicate our data to secondary "hot-spare" zones. In the event of a system or data loss, we can easily make use of backups for all components within our system. We have a thorough disaster recovery plan prepared in the event of any component failure or complete failure of our hosting provider.

Terms of Service

All accounts and subscriptions agree to our Terms of Service, which can be found at https://handwriting.io/terms-of-service/