SENTROPY

Sentropy Security & Privacy Overview

The content herein is correct as of October 2020 and represents the current state of security and data privacy at Sentropy at the time it was written. Sentropy's systems will evolve going forward, as we continually improve functionality for our customers.

INTRODUCTION

Security and privacy are fundamental to our mission, product development, and business. Our customers entrust us with keeping their users safe. We believe this starts by protecting the data from those users. This document provides you with information about our information security and data privacy practices.

Overview of Sentropy's interactions with customer data

- Sentropy is a SaaS company that provides tools and data to power content moderation and user safety applications. Our service offering consists of two products today:
    - **Sentropy Detect** is our API that receives content from customers and returns classifications of that content according to our taxonomy.
    - **Sentropy Defend** is our browser-based UI that allows customers to interact with those classification labels in various ways.
- Sentropy does not automatically moderate, edit, or alter any content on Customer's platform. We provide data that is meant to be reviewed by humans. Any decision to integrate our products to automate content moderation is yours and yours alone.
- We process the data you send to our API. If there is data in the end-user content that you don't want us to process, it is your responsibility to refrain from sending it to us.
- We don't share your data with anyone else.
- We improve our content classification algorithms in three ways.
    1. We learn from data and behavioral trends across the open web.
    2. We incorporate findings from manual investigations of the data you send to Sentropy Detect. Our data engineers will develop heuristics from the data you submit to our API. We use those heuristics to collect open data or programmatically generate synthetic data that we use to train our models. Customer data is never used to directly train our models.
    3. We use the actions you take in Defend to improve our understanding of how you classify content. These learnings apply to your instance only – they aren't shared with anyone else.
- Sentropy is a Processor of customer data under the GDPR and a Service Provider to customers under the CCPA.

Table of Contents

We Protect the Internet.

The online communities we visit every day establish norms quickly, shift frequently, and can degrade rapidly. As the space between online and offline life erodes, our devices become an extension of ourselves, and abuse becomes a very real-world issue.

Sentropy aims to end online abuse. Our platform supercharges content moderation to provide constantly evolving, unbiased detection models, allowing digital communities to seamlessly monitor, investigate, and protect the online spaces they care about the most. But providing state-of-the-art content safety technology necessitates care and investment on our part — it requires we follow the latest security best practices and comply with strict privacy regulations and corporate policies.

The information contained in this document is intended to provide transparency on Sentropy's security stance and processes. We also cover best practices gleaned from customer implementations to help you improve and secure the applications and communities you build with Sentropy.

Security Organization & Program

The Sentropy security framework is based on the AICPA's SOC 2 criteria and the ISO 27001 Information Security Standard and includes programs covering: Acceptable Use, Access Management, Backups, Business Continuity, Change Management, Code of Conduct, Cryptography, Incident Response, Information Security, Passwords, Responsible Disclosure, Risk Assessment, System Access Control, Vendor Management, and Vulnerability Management (together, the "Information Security Policies").

Security is represented at the highest levels of the company, with our executive management team meeting regularly to discuss issues and coordinate company-wide security initiatives. Information security policies and standards are approved by management and available to all Sentropy employees.

People Security

The people creating Sentropy's platform are important; we've implemented processes to ensure we're bringing in the right people and keeping them up-to-date on the latest security trends. Here are some of the processes we have in place:

Background Checks

All candidates in the U.S. must pass stringent background checks by a specialized third-party before being offered a position. For domestic candidates, these checks include: SSN trace, national, federal, and county criminal searches, National Sex Offenders Public Registry, and OFAC. We use the same approach for international new hires, but make any changes necessary to comply with local laws. In all cases, we conduct extensive reference checks for candidates before any offers are delivered.

InfoSec Training

All new Sentropy employees are required to complete security training during the onboarding process. In addition, all Sentropy employees must take security and privacy training once a year, which covers our Information Security Policies, security best practices, and privacy principles.

Employee and Contractor Offboarding

All employees and contractors are fully offboarded within 24 hours of termination. This process includes a review of the individual's recent activity on Sentropy's systems, access termination to each system, and the return of all hardware to the Company.

PRODUCT SECURITY

The mission of Sentropy's Product Security program is to enable our engineering and product teams to build solutions that are best-in-class when it comes to security. The following activities help us to achieve this mission:

Secure by Design

Sentropy engineers continuously perform numerous activities to ensure that our products and data are secure, including:

- Internal code reviews before products are launched or product updates are deployed;
- Regular penetration tests performed by third-party specialists;
- Quarterly vulnerability tests; and
- Reviews of vulnerabilities surfaced through internal testing and our Responsible Disclosure Program.

Restricted Access

Our production systems and database infrastructure are accessible only to those employees who require access to improve our product and service. Our application environment and internal tools are protected by a virtual private cloud. Users must authenticate API requests using a unique key tied to each customer account. Sentropy also enforces a strict password policy that applies to all of our employees and contractors.

Customer Data Segregation

We keep each customer's raw data logically separate from that of other customers. Our systems were built to ensure that customers may never view other customers' private data.

Change Management

Sentropy has a formal change management process where all changes are tracked and are approved. A change is reviewed before being moved into a staging environment where it is further tested before finally being deployed to production. A limited number of Sentropy employees have the ability to approve and deploy changes to production code.

Encryption At-Rest and In-Transit

Sentropy supports TLS 1.2 to encrypt network traffic between the customers and Sentropy. All data on Sentropy's servers is encrypted at-rest.

Penetration Testing

Sentropy performs annual third-party penetration tests. Additionally, our responsible disclosure program encourages ongoing testing and responsible disclosure of vulnerabilities from the security community.

Cloud & Network Infrastructure Security

The security of our infrastructure and networks is critical. Creating a safe platform for Sentropy applications and customer innovation is the mission of our cloud security program. Our cloud and network infrastructure security are driven by four key principles:

Asset Management and Ownership
All cloud assets must have a defined owner, security classification, and purpose.

Infrastructure Management
Direct access to infrastructure, networks, and data is minimized to the greatest extent possible. Where possible, control planes are used to manage services running in production, to reduce direct access to host infrastructure, networks, and data. Direct access to production resources is restricted to employees requiring access and requires approval, strong multifactor authentication, and access via a proxy.

Continuous Monitoring and Vulnerability Management

At Sentropy, the security and resiliency of our products and infrastructure is a top priority. Our continuous monitoring approach builds on industry-standard principles that drive us to develop processes and procedures for leading incidents and designing proactive and detective capabilities for the Sentropy Platform. Through the ongoing awareness of vulnerabilities, incidents, and threats, Sentropy is poised to respond and mitigate accordingly.

Continuous Monitoring Program
Sentropy approaches continuous monitoring through the development of proactive and detective capabilities. Through the ongoing awareness of vulnerabilities, incidents, and threats, Sentropy is poised to respond and mitigate accordingly.

Incident Response Program
Sentropy maintains an incident response program. The program defines conditions under which security incidents are classified and triaged. Sentropy's Security Team assesses the threat of all relevant vulnerabilities or security incidents and establishes remediation and mitigation actions for all events.

Security Log Retention
Security logs are retained for 12 months. Access to these security logs is limited to the Sentropy employees on a need-to-know basis.

Physical Security

Physical security is an important part of Sentropy's security strategy. We're committed to securing our facilities.

Datacenter Security
Sentropy leverages Google Cloud Platform (GCP) data centers for all production systems and customer data. GCP follows industry-best practices and complies with an impressive array of standards.

For more information on GCP, see the Google Infrastructure Security Design Overview.

Office Location Security
Sentropy has a security program that manages visitors, building entrances, CCTVs, and overall office security. All employees, contractors and visitors are required to wear identification badges which distinguish their respective role. Sentropy's office resides in a building with 24x7 security.

Third-Party Security

In today's interconnected business environment, maintaining visibility into the software supply chain is of utmost importance. Sentropy has implemented the following programs:

Vetting Process
Third parties used by Sentropy are assessed before onboarding to validate that prospective third parties meet Sentropy's security requirements.

Ongoing Monitoring
Once a relationship has been established, Sentropy periodically reviews security and business continuity concerns at existing third parties. The program takes into account the type of access and classification of data being accessed (if any), controls necessary to protect data, and legal or regulatory requirements.

Offboarding
Sentropy ensures that data is returned and/or deleted at the end of a vendor relationship.

Security Compliance

Sentropy is committed to mitigating risk and ensuring Sentropy services meet regulatory and security compliance requirements:

Regulatory Environment
Sentropy complies with applicable legal, industry, and regulatory requirements as well as industry best practices.

Top-Tier Infrastructure Provider
Sentropy's cloud communications platform is hosted at Google Cloud Platform (GCP) data centers, which are highly scalable, secure, and reliable. GCP complies with leading security policies and frameworks, including SOC framework, ISO 27001, and PCI DSS.

ISO 27000 Series
Sentropy's information security management system is aligned with ISO/IEC 27001:2013 principles, showing our maturity within the Information security space. Security is a top priority for Sentropy, and our alignment with ISO 27001 principles demonstrates our commitment to information security, data protection, and continuous improvement as we continue to evolve and improve all aspects of our data security practices.

SOC 2
Sentropy is SOC 2 Type 1 compliant, and is preparing to begin its audit for its SOC 2 Type 2 certificate (expected to be completed in Q1 2021).

DATA PRIVACY

As a data processor, adhering to local regulations is only one component of our commitment to privacy. Our higher order mission is to treat you and your customers with the respect you deserve.

Data Collection and Processing
There are three core types of data that Sentropy collects: (a) customer data, which is any data submitted via our APIs; (b) metadata; and (c) data related to actions taken through Sentropy Defend, our workflow tool.

- *Customer data* sent through Sentropy's APIs are securely stored in internal Kafka queues and replicated in internal Sentropy databases. We routinely sample limited volumes of customer data to evaluate the quality of our models; all such data is stored in customer-specific Google Cloud Storage (GCS) buckets or internal databases that are accessible only to those of our employees that require access for quality testing. Customer data is retained for a maximum of 90 days or for the duration during which the customer data satisfies the import criteria of Sentropy Defend, whichever is longer. Customers can elect to have this data deleted at any time, although doing so may limit the functionality of Sentropy Defend. We don't automatically identify passwords or

personal data and we very strongly recommend you take precautions to avoid submitting this type of data to our API endpoints.

- *Metadata* includes data related to API keys, authentication and data derived from customer data submitted to our API. Derived data does not include any customer data. All metadata is kept separate from customer data you send. Customer login passwords for the Sentropy application are salted and hashed using the industry standard bcrypt. All metadata is backed up daily to avoid data loss and service disruption, and is stored in GCS indefinitely.
- *Sentropy Defend data* includes the data related to actions you take through Sentropy Defend, our workflow tool. This data is securely stored indefinitely in GCS.

All customer data stored in GCS is logically partitioned by the ID of the data source, and access is controlled via IAM permissions. Data in GCS is encrypted at rest using Google's GKE offering.

Annual Privacy Training
All Sentropy employees are required to undergo annual privacy training to ensure awareness of Sentropy's role in protecting end-user and customer data privacy.

Data Processing Agreement
Our Data Processing Agreement (DPA) reflects the requirements of the GDPR.

Data Transfer Practices
Sentropy is certified under the EU-U.S. and Swiss-U.S. Privacy Shield Frameworks for user data transfer and storage as a part of our commitment to comply with EU data protection requirements when transferring personal data from the European Union to other countries and regions. Where we engage subprocessors, we impose data protection terms on the subprocessors that provide at least the same level of protection for Personal Data as those in our DPA including, where appropriate, the Standard Contractual Clauses.

Privacy by Design
Your data is yours to own. Sentropy does not sell our customers' user data.

Privacy Policy
Our Privacy Policy honors CCPA, the GDPR, EU-U.S. and Swiss-U.S. Privacy Shield Frameworks.

Data Protection Officer
Sentropy has appointed an independent Data Protection Officer to oversee our ongoing compliance efforts.

SUMMARY

Sentropy's content moderation platform enables businesses to provide the community experiences their users expect by easily incorporating powerful moderation technologies and content intelligence into their products and Trust & Safety workflows. Security mechanisms to protect physical, network, and application components of the platform, coupled with transparency about security, compliance, and data privacy practices, give customers the confidence they need to fight abuse and malicious content at scale.

If you have more questions, or need more detailed answers, feel free to get in touch with our Security Team at security@sentropy.com.