Heap, Inc.

System and Organization Controls Report (SOC 3)

Independent Report of the Controls to meet the criteria for the Security, Availability, and Confidentiality categories for the period of March 1, 2021 through February 28, 2022.

KirkpatrickPrice

4235 Hillsboro Pike
Suite 300
Nashville, TN 37215

TABLE OF CONTENTS

ASSERTION OF HEAP, INC. MANAGEMENT 1
INDEPENDENT SERVICE AUDITOR'S REPORT 3
Scope 4
Service Organization's Responsibilities 4
Service Auditor's Responsibilities 4
Inherent Limitations 5
Opinion 5
HEAP, INC.'S DESCRIPTION OF ITS SOFTWARE-AS-A-SERVICE SYSTEM 6
Section A: Heap, Inc.'s Description of the Boundaries of its Software-As-A-Service System . 7
Services Provided 7
Client Engagement and Platform Functionality 7
Locations 8
Infrastructure 8
Software 9
People 10
Data 10
Processes and Procedures 11
Section B: Principal Service Commitments and System Requirements 13
Contractual Commitments 13
System Design 13

ASSERTION OF HEAP, INC. MANAGEMENT

ASSERTION OF HEAP, INC. MANAGEMENT

We are responsible for designing, implementing, operating, and maintaining effective controls within Heap, Inc.'s Software-as-a-Service system (system) throughout the period March 1, 2021, to February 28, 2022, to provide reasonable assurance that Heap, Inc.'s service commitments and system requirements relevant to Security, Availability, and Confidentiality were achieved. Our description of the boundaries of the system is presented in section A and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period March 1, 2021, to February 28, 2022, to provide reasonable assurance that Heap, Inc.'s service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability, and Confidentiality (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*). Heap, Inc.'s objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in section B.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

We assert that the controls within the system were effective throughout the period March 1, 2021, to February 28, 2022, to provide reasonable assurance that Heap, Inc.'s service commitments and system requirements were achieved based on the applicable trust services criteria.

INDEPENDENT SERVICE AUDITOR'S REPORT

Ken Fine
CEO
Heap, Inc.
225 Bush Street, Suite 200
San Francisco, CA 94104

Scope

We have examined Heap, Inc.'s accompanying assertion titled "Assertion of Heap, Inc. Management" (assertion) that the controls within Heap, Inc.'s Software-as-a-Service system (system) were effective throughout the period March 1, 2021, to February 28, 2022, to provide reasonable assurance that Heap, Inc.'s service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability, and Confidentiality (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

Service Organization's Responsibilities

Heap, Inc. is responsible for its service commitment and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that Heap, Inc.'s service commitments and system requirements were achieved. Heap, Inc. has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Heap, Inc. is responsible for selecting, and identifying in its assertion, the applicable trust services criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

Service Auditor's Responsibilities

Our responsibility is to express an opinion, based on our examination, on whether management's assertion that controls within the system were effective throughout the period to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Our examination included:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements
- Assessing the risks that controls were not effective to achieve Heap, Inc.'s service commitments and system requirements based on the applicable trust services criteria

- Performing procedures to obtain evidence about whether controls within the system were effective to achieve Heap, Inc.'s service commitments and system requirements based on the applicable trust services criteria

Our examination also included performing such other procedures as we considered necessary in the circumstances.

Inherent Limitations

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Opinion

In our opinion, management's assertion that the controls within Heap, Inc.'s Software-as-a-Service system were effective throughout the period March 1, 2021, to February 28, 2022, to provide reasonable assurance that Heap, Inc.'s service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

Joseph Kirkpatrick
CPA, CISSP, CGEIT, CISA, CRISC, QSA
4235 Hillsboro Pike, Suite 300
Nashville, TN 37215

April 25, 2022

HEAP, INC.'S DESCRIPTION OF ITS SOFTWARE-AS-A-SERVICE SYSTEM

SECTION A:
HEAP, INC.'S DESCRIPTION OF THE BOUNDARIES OF ITS SOFTWARE-AS-A-SERVICE SYSTEM

Services Provided

Founded in 2013, Heap provides an analytics platform to its clients that allows them to capture data about how their customers use their products. The Heap platform is designed to allow the organization's clients to understand how people interact with their product, increase acquisition and retention, reduce engineering burden, and create a powerful product experience. With the Heap platform, the organization's clients are able to map out their product and establish meaningful key performance indicators (KPIs) at all levels, which can be used to measure the impacts of decisions, isolate problem areas, prioritize efforts, and tie granular activities to high-level business metrics.

Client Engagement and Platform Functionality

Paying clients are typically initially taken through a guided onboarding exercise. During onboarding, clients receive training for effective use of the Heap analytics product to fully exploit its retroactive analysis capabilities enabled through automatic capture of user behavioral data. Onboarding typically also includes assistance in the initial setup of the account, permissions, and definitions.

Clients access the front end of Heap's software-as-a-service (SaaS) via the organization's website and mobile application. Clients can view event data, define events, and perform analysis. The product can integrate with client's webpages, android applications, and iOS apps. Event listeners integrate with the clients application to ingest event data and send to Heap for processing. Event data is correlated with a user identity and stored in a PostgreSQL database cluster.

When onboarding new clients, the Marketing and Sales Development teams work to qualify leads and then hand the leads off to a Sales Representative. The Sales team does an initial discovery call and if the client wishes to proceed, the team hands them off to a Solutions Consultant. The Solutions Consultant then demonstrates the product, performs a technical validation, and sets up a proof of value installation of the product. This can be installed in the client's web or mobile application or it can be set up with test data. If installed in the client's application, the steps used are similar to the normal onboarding process. Each step in the process is documented in Salesforce.

Clients negotiate with legal and finance and then sign a contract. The record in Salesforce is updated, which triggers a message in Slack to notify the Technical team who begins onboarding. The Solutions Consultant has a hand off call with the Technical team to initiate the onboarding process.

The organization's SaaS platform has a free trial feature, which is also used to onboard paying clients. The client self-enrolls, creates an account, and receives a welcome email with links to provide a guided experience on how to install. This process creates an account number that is associated with the client. If the client is using a web page, they follow instructions to add a

JavaScript to their page. If using mobile applications, there are different software development kits (SDKs).

Auto-capture functionality is enabled on websites by placing a standard tracking script in the header, and for mobile applications, specific build-steps are integrated to compile in the auto-tracking code.

After data capture has started, the Event Visualizer can be used to interactively define relevant virtual events based on interactions with elements of the site/application. Virtual events can retroactively incorporate all user interactions back to the data retention limit or when the auto-capture was installed, whichever is the more recent. Heap offers the ability to export data to client's data warehouses. If the client requests the ability to export, then their data is copied to S3 hourly where they can access via a cross account role in AWS to pull data to their warehouse. Supported warehouses include BigQ, Redshift, Snowflake, and S3.

The user interface to the Heap software provides capabilities to perform graphing and funnel analysis over aggregate behavioral data. Graphs can also be collected in dashboards to monitor related relevant metrics in a single screen, and Heap allows for live outbound data-warehouse syncs where behavioral data can be further analyzed with dedicated BI tools.

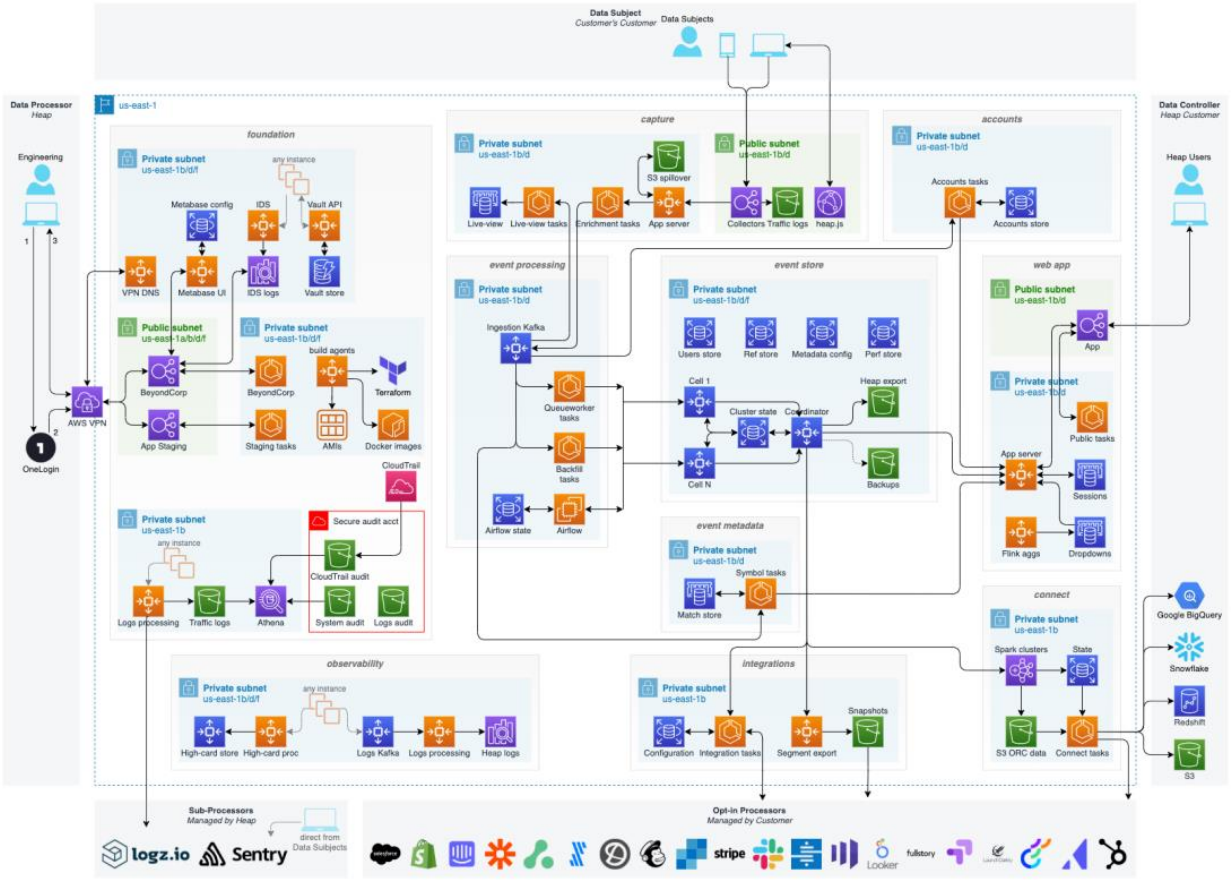
Security commitments are dependent upon the client's needs. Heap proactively shares SOC 2 and Health Insurance Portability and Accountability Act (HIPAA) audits, and for most companies, this is sufficient. For mid-market companies, the organization requires completion of a security review and questionnaire. Enterprise-level customers often have more in-depth reviews and audits.

Locations

The San Francisco, California and New York, NY locations are in scope for this audit.

Infrastructure

The organization documents its network design for the purpose of showing its network inter-connectivity between its locations and the associated segmentation of various parts of network and perimeter security of its network via firewalls. To outline the topology of its network, the organization maintains the network diagram below to illustrate its internal infrastructure. The Bedrock Engineering team is responsible for maintaining the network diagram for the AWS environment.



In addition, the organization maintains an inventory of production systems in AWS via the AWS console. Workstation inventory is maintained via Jamf.

Software

The organization maintains an inventory of software in AWS via the AWS console. All other critical software is tracked manually. The following software is used in the development of Heap's SaaS platform:

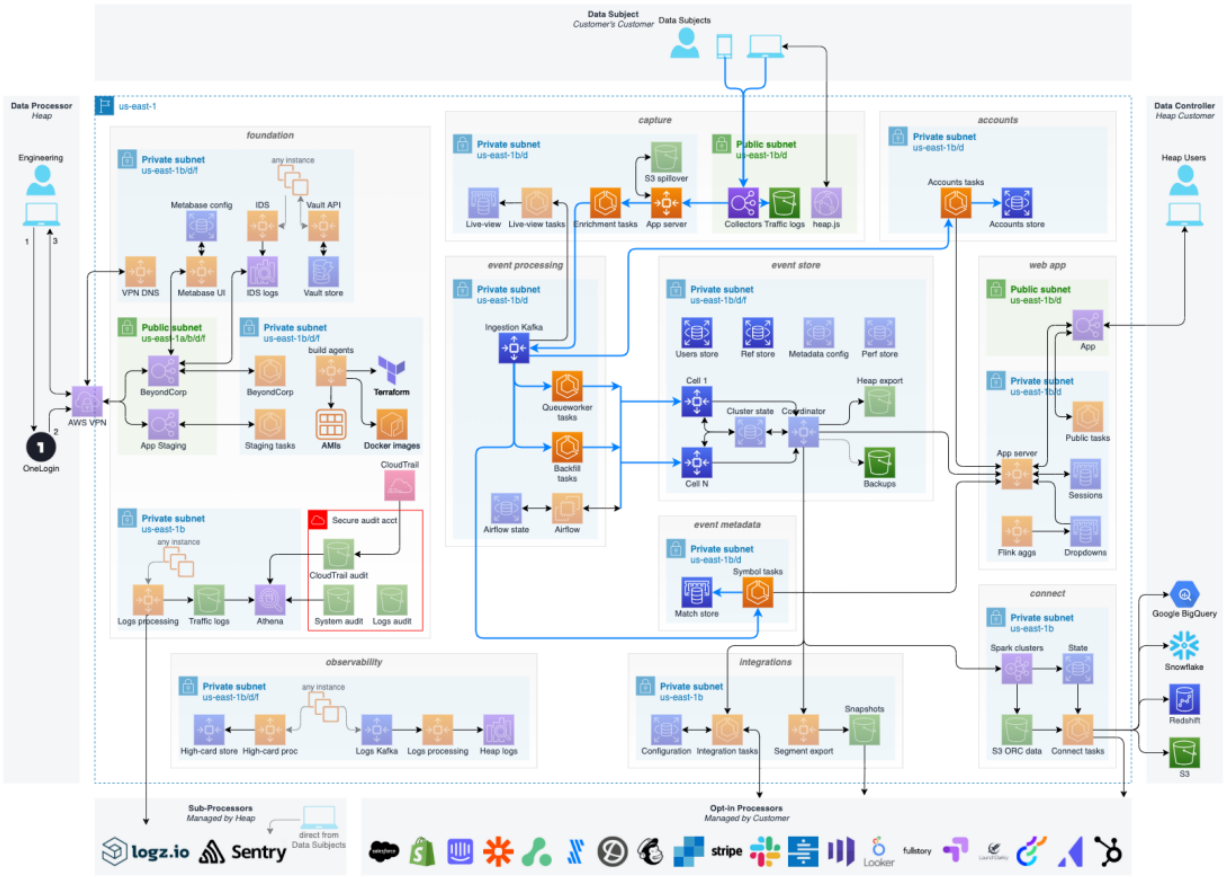
- AWS
- Datadog
- Foxpass
- HelloSign
- Logz.io
- PagerDuty
- Salesforce
- SendGrid
- Slack
- Statuspage
- Wazuh
- Zoom

People

Heap has a traditional hierarchical structure with the CEO at the head of the organization. The organization is divided into seven departments led by department heads that report to the CEO. Security and Compliance personnel have a direct reporting to management to maintain independence. The organization also has a seven-member Board of Directors that is comprised of the two co-founders and five independent parties. The main function of the board is to provide oversight regarding financial health and strategic direction for Heap. To outline its hierarchical structure, Heap maintains an organization chart, which has been summarized below to show the CEO and direct reports.

Data

To provide its services, the organization stores, processes, and transmits customer data as well as Heap business data and source code data. Data captured in Heap's system is intrinsically designed to be robust. The public capture application programming interface (API) by design must capture any and all traffic that hits it. Once data is captured it is immediately stored in a fully redundant Kafka cluster for downstream processing. Access to captured data for a given customer is tied internally to a unique "app_id" tied to the user login via the customer account. The system pervasively ensures that a given session can only ever access data captured and associated with the correct "app_id" as a baseline data safety measure to avoid misrouting. The requests Heap handles from its customers involve requesting aggregate analytics over the captured end-user interactions within their sites and are intrinsically not susceptible to malicious subversion by any of the mentioned means. The organization maintains a data flow diagram to illustrate this flow of sensitive data throughout the environment. The Bedrock Engineering team is responsible for maintaining the diagram for the AWS environment.



In addition, the organization documents requirements for the handling of sensitive customer information. Detection algorithms are in place to detect and purge sensitive data that is collected incidentally. All confidential information transmitted via the internet is encrypted in transit using Transport Layer Security (TLS) v1.2 or higher by all systems. Heap uses the following technologies to assist in securing all transmissions over the internet:

- HashiCorp Vault for secret management within production
- AWS Certificate Manager for public TLS certificates
- Public internet-facing load balancers configured according to AWS best practices

For payment processing, the organization uses Zuora to facilitate payments from customers.

Processes and Procedures

Management has developed and communicated procedures to guide the provision of the organization's services. Changes to procedures are performed annually and authorized by management. These procedures cover the following key security life cycle areas:

- Data classification
- Categorization of information
- Assessment of the business impact resulting from proposed security approaches
- Selection, documentation, and implementation of security controls
- Performance of annual management self-assessments to assess security controls

- Authorization, changes to, and termination of information system access
- Monitoring security controls
- Management of access and roles
- Maintenance and support of the security system and necessary backup and offline storage
- Incident response
- Maintenance of restricted access to system configurations, user functionality, master passwords, powerful utilities, and security devices

SECTION B:
PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

Contractual Commitments

Heap executes contracts with its clients that describe the scope of services offered. Contracts vary depending on the size of the company, but all contracts link directly to Heap's website, which includes Heap's Terms of Service. Standard contracts do not include service level agreements (SLAs). However, a pre-defined set of SLAs can be added upon request for certain categories of clients. Heap's service availability to customers is 99.5% of all scheduled availability, which is calculated annually. The organization also uses marketing materials published on its website to communicate the services it offers. The organization designs its security programs and business operations to maintain compliance with industry expectations and regulatory commitments.

System Design

Heap designs its data capturing services system to meet its regulatory and contractual commitments. These commitments are based on the services that Heap provides to its clients, the laws and regulations that govern the provision of those services, and the financial, operational, and compliance requirements that Heap has established for its services. Heap establishes operational requirements in its system design that support the achievement of its regulatory and contractual commitments. These requirements are communicated in Heap's system policies and procedures, system design documentation, and contracts with clients.