REPORT ON ALGOLIA, INC.'S SEARCH SOLUTION SYSTEM RELEVANT TO SECURITY, AVAILABILITY AND CONFIDENTIALITY FOR THE PERIOD JULY 1, 2017 TO DECEMBER 31, 2017

SOC for Service Organizations - SOC 3

COALFIRE CONTROLS

TABLE OF CONTENTS

SECTION 1

Independent Service Auditor's Report 3

SECTION 2

Algolia, Inc.’s Assertion 6

SECTION 3

Management’s Description of the Boundaries of Algolia, Inc.’s Search Solution System 8

SECTION 1

INDEPENDENT SERVICE AUDITOR'S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

To the Management of Algolia, Inc. ("Algolia"):

Scope

We have examined Algolia's accompanying assertion titled "Assertion of the Management of Algolia, Inc." (assertion) that the controls within Algolia's Search Solution System (System) were effective throughout the period July 1, 2017 to December 31, 2017, to provide reasonable assurance that Algolia'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 100A *Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (2016 AICPA, *Trust Services Criteria*).

Service Organization's Responsibilities

Algolia is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the System to provide reasonable assurance that Algolia's service commitments and system requirements were achieved. Algolia has also provided the accompanying assertion about the effectiveness of controls within the System. When preparing its assertion, Algolia is responsible for selecting, and identifying in its assertion, the applicable trust service 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 Algolia'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 Algolia'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 Algolia's Search Solution System were effective throughout the period July 1, 2017 to December 31, 2017, to provide reasonable assurance that Algolia's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

Coalfire Controls LLC

March 30, 2018
Coalfire Controls, LLC

SECTION 2

ALGOLIA, INC.'S ASSERTION

algolia

Assertion of the Management of Algolia, Inc. ("Algolia")

We are responsible for designing, implementing, operating and maintaining effective controls within the Search Solution System (System) throughout the period July 1, 2017 to December 31, 2017, to provide reasonable assurance that Algolia'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 3 of this report 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 July 1, 2017 to December 31, 2017, to provide reasonable assurance that Algolia'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 100A, Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (2016 AICPA, Trust Services Criteria). Algolia'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 3 of this report.

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.

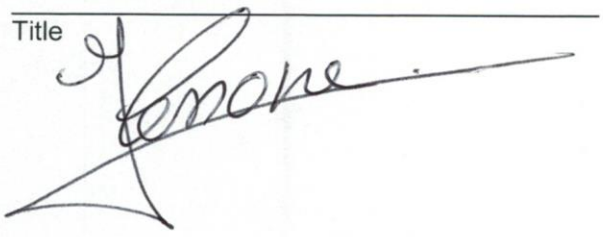
We assert that the controls within the system were effective throughout the period July 1, 2017 through December 31, 2017, to provide reasonable assurance that Algolia's service commitments and system requirements were achieved based on the applicable trust services criteria.

Julien Lemoine

Algolia, Inc. Authorized Representative

CTO & Co-Founder

Title



Signature of Authorized Representative

SECTION 3

DESCRIPTION OF THE BOUNDARIES OF ALGOLIA, INC.'S SEARCH SOLUTION SYSTEM FOR THE PERIOD JULY 1, 2017 TO DECEMBER 31, 2017

OVERVIEW OF SERVICE PROVIDED

Since 2014, Algolia, Inc. (“Algolia” or “the Company”) has provided its Search Solution System to businesses of all sizes around the world. Algolia provides user entities (customers) a hosted and internally developed search solution to provide an end-to-end search experience for their applications and services.

The scope of services covered in this report includes the following components of the Search Solution System:

Algolia Search API

Algolia Search Application Programming Interface (API) is the internally developed proprietary core of Algolia’s services. Algolia Search API provides up to 99.999% availability which is achieved by its distributed nature.

In order to mitigate the impact of network latency, Algolia Search API provides an option of enriching the primary cluster by an arbitrary number of Distributed Search Network (DSN) servers that serve as read replicas. The users are then geo-routed to the closest server having the customer data. Besides lowering network latency, this solution also improves the availability of the whole system by making it more resilient to region scale outages.

Algolia Dashboard

Algolia Dashboard is a web management interface that uses the Algolia Search API and provides a user-friendly interface for using and configuring the Search API. The dashboard also provides user-management functionality.

Algolia Analytics API

Algolia Analytics API is a JSON-based API that provides access to analytics data generated from the queries. The queries performed through the Algolia Search API are collected, analyzed, and made available through this API allowing the customer to analyze the user experience, trends, and impacts of changes.

Algolia Monitoring API

Algolia Monitoring API is an abstraction API for Algolia’s multiple monitoring systems that collects data about the usage and operations of the Algolia Search API. This API allows customers to get the data that is available in the Algolia Dashboard and is used for the Algolia status page.

Algolia Places API

Algolia Places API is a geo-data service based on Algolia Search API that Algolia provides to its customers to address auto-complete in a search-only mode where the dataset is constructed and managed by Algolia.

Algolia Offline Search

Algolia Offline Search provides a functional offline search for mobile applications. Algolia Offline Search works together with the Algolia Search API for data synchronization and is provided as a binary library for mobile platforms.

THE COMPONENTS OF THE SYSTEM USED TO PROVIDE THE SERVICES

INFRASTRUCTURE

Algolia operates its services on a physical and virtual infrastructure placed in third party datacenters and colocation services of third party server providers. The data centers hosting the services are located in US West (California), US Central (Dallas area), US East (Virginia), Canada (Montreal area), South America (São Paulo), Europe (France, Netherlands and Germany), Russia (Moscow), South Africa, India, Singapore, Hong Kong, Japan (Tokyo and Osaka), and Australia (Sydney). Portions of the provided services are hosted by various cloud providers, namely OVH, Amazon Web Services (AWS) and Google Cloud Platform.

In order to increase the overall security of the system, Algolia has designed its network environment as a Zero-Trust Network with traditional network concepts of external untrusted and internal trusted networks, but without a DMZ network. In Algolia's environment, all the networks are external untrusted and each of the two servers need to be authorized to communicate together internally. Algolia's environment spans multiple data centers, multiple service providers, and multiple network autonomous systems while maintaining the security, resiliency, and availability of the service.

Algolia also operates the related network equipment (located in-house) that supports the infrastructure located at colocation provider facilities.

SOFTWARE

The environment of Algolia is based on Linux operating systems and heavily utilizes open-source software. Algolia's environment is composed of multiple systems offering the services to its customers which work in tandem with internal systems supporting the operations of the infrastructure.

Internal Systems

Application Monitoring

Algolia uses multiple monitoring systems with redundant architectures including Pingdom, host-based monitoring and its own purpose-built monitoring network. While Pingdom provides a high level overview of system availability, Algolia's purpose-built monitoring network provides telemetry data about the availability of its services. This network is composed of multiple monitoring probes running around the world and constantly monitoring the Algolia infrastructure and its services. This data is then exposed live on Algolia's public automatic status page. No human intervention is necessary for the status page to display that the service is degraded or unavailable and all the data is also available in the monitoring API.

The application monitoring system also verifies the correctness of Algolia's services by performing end-to-end logic tests of the services. Algolia's monitoring network also monitors critical portions of the infrastructure, such as Domain Name Server (DNS) service endpoints of Algolia's providers.

Infrastructure Monitoring

Every system in the Algolia environment is monitored, including infrastructure metrics such as central processing units (CPU), memory, and network utilization. This data is then transparently collected and analyzed. Additional alerts are evaluated on top of this data to provide Algolia with pro-active alerting that might impact the service before the actual degradation happens.

Backups and Disaster Recovery

Algolia has developed internal backup mechanisms that mirror the application data multiple times per day from the production servers to backup locations over an encrypted tunnel. Once the mirror is finished, a local processing of the data is performed, and consistency of the data is verified before further processing. Then an encrypted backup is generated and distributed to the recovery storage closest to the source cluster in order to provide the fastest possible recovery times.

Logging

Algolia collects and maintains detailed logs from both the infrastructure and application level. These logs are centrally collected, analyzed, and respective alerts are evaluated. The collection of the logs is automatic. Additional application specific collections are configured either by the Configuration Management tool or implicitly by producing the logs to Syslog.

Patch Management

All Algolia servers and the running software are regularly patched. If the particular software allows it, automatic updates are enabled and security updates are installed automatically without intervention.

Integrity Monitoring

Algolia uses a Host-Based Intrusion Detection System (HIDS) to ensure file integrity and protection of the systems from intrusion. The HIDS performs integrity tests of important files of the system and reports any changes. The HIDS uses its known signatures to regularly scan the systems for rootkits and other malware. HIDS alerts are centrally collected and analyzed.

PEOPLE

The development and operations of the systems are the responsibility of the Research & Development organization unit of Algolia, which is led by the Chief Technology Officer (CTO) and Vice President (VP) of Engineering.

Engineering teams working on particular systems are given the necessary infrastructure and tools they need for system development, testing, and operations. These teams operate their systems on their own and are responsible for the availability and operations of the system.

The engineering team led by the Director of Infrastructure works on the automation, maintenance, operations, and security of all systems in Algolia. This engineering team also includes Algolia’s Security Team who is responsible for developing and designing the secure practices of Algolia systems, performing internal training, and developing new systems to improve the overall security of Algolia.

The Product team leads the development of Algolia’s services based on the feedback from customers, market needs, and future visions of Algolia.

The Director of Infrastructure, CTO, VP of Engineering, and Head of Legal ensure Algolia’s continuous compliance with all developed policies and legal requirements.

Human Resources (HR) of Algolia contributes to the security of Algolia’s systems by performing background checks on new employees, adding new employees to Active Directory, and revoking assigned rights during the termination process.

PROCEDURES

Algolia utilizes automation for all its systems to help achieve security, recovery from failures, administration, and provide an overview of its assets. In order to ease the adoption of internal policies and guide employees through the correct processes, Algolia encompasses as much as possible into internal applications, configuration management, and internal systems.

Algolia has developed policies covering the needs of operations and nature of services provided. These policies are available to all employees of the Company, business partners, and customers. Each policy is versioned and changes are logged.

The default system and server security configurations of all Algolia systems are anchored in the configuration management system based on the Chef configuration management tool that reconfigures the system to a desired state using predefined and dynamic templates. The configuration management system also provides the functionality of service discovery allowing Algolia to operate its systems in a Zero-Trust architecture.

The Change Management policy governs how changes are made to production. Most of the changes are performed by changing code or configurations in system-related Git code repositories. These changes are tested in testing environments, approved by an engineering peer, and then deployed to production. Algolia employs multiple methods of production software deployment depending on the criticality of the system including: cold restart, hot reload, blue-green deployment, canary deployment, gradual deployment based on service type, and regional deployment.

The automatic monitoring system has the ability to trigger critical alerts and notify the 24/7 on-call team in order to resolve immediate issues and restore service. The most critical applications, like Algolia Search API, have the ability to trigger alerts directly without the monitoring system if the monitoring system is unavailable.

DATA

Algolia's business does not sell customer data and Algolia has developed an environment that protects the data and confidentiality of its customers.

Data Classification

Algolia has developed a Data Classification Policy for both customers and its own data. Due to the implicit sensitivity of customer data, this data is classified as "confidential".

Algolia Search API

Algolia search API works with semi-structured JSON formatted objects received via REST API. This API is available via HTTP for legacy systems and HTTPS for modern systems, with industry best practice TLS configuration and certificates from respected public certification authorities. This API follows HTTP standards and it's usable as is or through integration libraries that Algolia provides as an open source software.

Algolia Dashboard

Algolia Dashboard is a web application primarily built on top of the Algolia Search API that provides additional user management and authentication for management. Algolia Dashboard stores information about authorized users which were added by the customer.

Algolia Analytics API

Algolia Analytics API does not handle customer data records. Analytics API produces data generated from the usage and audit logs of the Algolia Search API. This allows customers to get visibility into search requests being performed by their systems or their users.

Algolia Monitoring API

Algolia Monitoring API does not handle customer data. Monitoring API produces data collected from Algolia about the state of the service and makes that information available to customers.

Algolia Places API

Algolia Places API contains a preconfigured dataset and as such does not allow data to be stored.

Logging

All systems produce application and operations logs which are collected, processed, and stored in Algolia's systems. These logs are purged from the system following its retention requirements.

Data retention

When data is being requested for deletion via the API, it is made unavailable as soon as the system converges and marks the data as ready for garbage collection (data purge). During the next garbage collection, the data is purged from the system by removing the data from its data storage and thus making it unavailable. At this point, the data is no longer accessible to the customer or Algolia, cannot be restored, and will not be listed by any of the tools or APIs.

After the backup retention period expires, the data is also purged from the backup systems. All Algolia systems are designed to automatically remove data marked for deletion in a timeframe specified by the internal Data Retention and Disposal Policy.

Algolia has established processes to allow customers to request data to be deleted from all systems.

THE BOUNDARIES OF THE SYSTEM COVERED BY THE DESCRIPTION

This report includes the Algolia Search Solutions System. Any other Algolia services are not included within the scope of this report.

The boundaries of the system are the specific aspects of the Company's infrastructure, software, people, procedures, and data necessary to provide its services and that directly support the services provided to customers. Any infrastructure, software, people, procedures and data that indirectly support the services provided to customers are not included within the boundaries of the system.

The Company uses a variety of subservice organizations for data center, data center colocation, server hosting, and cloud services. The description of the boundaries of the system only cover the Trust Services Principles and Criteria and related controls of the Company and exclude the related controls of these subservice organizations. Although subservice organizations have been carved out for the purposes of this report, certain controls are expected to be in place related to physical security and environmental protection.

The Company relies on the following subservice organizations to provide data center, data center colocation, server hosting, and cloud services: Amazon Web Services, Google, Equinix, Leaseweb, OVH, IPTP, Anexia, Internap, Packet, Maxihost, Hetzner, Zone Networks, WAN Security, E2E Networks and Web Werks.

COMMITMENTS AND SYSTEM REQUIREMENTS

COMMITMENTS

Commitments are declarations made by management to customers regarding the performance of the Algolia Search Solutions System. Commitments are communicated in written individualized agreements, standardized contracts, service level agreements (SLAs), or published statements. Standard agreements are available on Algolia's public website and specific agreements are part of the individual contracts with customers. The Company's commitments include the following:

- Scope of the provided services
- Required service level agreements
- Required level of support
- Used confidentiality and security standards
- Availability of the services

SYSTEM REQUIREMENTS

System requirements are specifications regarding how the Algolia Search System should function to meet the Company's commitments to customers. Requirements are specified in the Company's policies and procedures, which are available to all employees. The Company's system requirements include the following:

- Employee provisioning and deprovisioning standards
- Logical access controls such as use of user IDs and passwords to access systems
- Risk assessment standards
- Change management controls
- Incident response
- Monitoring controls

AVAILABILITY

The availability principle refers to the accessibility of the system or services as committed by the Company's service agreements. The availability of Algolia Search System is dependent on many aspects of the Company's operations including failures that are outside of Company's systems or outside of Company's powers to influence. The risks that would prevent the Company from meeting its availability commitments and requirements are diverse. Availability includes consideration of risks during normal business operations, during routine failure of elements of the system, as well as risks related to the continuity of business operations during a natural or man-made disaster.

The Company has designed its controls to address the following availability risks:

- Insufficient processing capacity.

- Insufficient Internet response time.
- Loss of processing capability due to a power outage.
- Loss of communication with user entities due to a break in telecommunication services.
- Loss of key processing equipment, facilities, or personnel due to a natural disaster.

In evaluating the suitability of the design of availability controls, the Company considers the likely causes of data loss, the commitments and requirements related to availability, the timeliness of back-up procedures, the reliability of the back-up process, and the ability to restore backed-up data. In evaluating the design of data availability controls, the Company considers that most data loss does not result from disasters but, rather, from routine processing errors and failures of system elements.

CONFIDENTIALITY

The confidentiality principle addresses the system's ability to protect information designated as confidential, including, its final disposition and removal from the system in accordance with management's commitments and system requirements. Information is confidential if the company that holds or stores information is required to limit its access, use, and retention, and restrict its disclosure to defined parties (including those who may otherwise have authorized access within the boundaries of the system).

The confidential information that the Company maintains includes customer data and other information that customers communicate to the Company during the ordinary course of business.

The Company has designed its controls to address the following confidentiality risks:

- Data used in nonproductive environments is not protected from unauthorized access.
- Unauthorized access to confidential information is obtained during processing.
- Confidential information is transmitted to related parties, vendors, or other approved parties contravening confidentiality commitments.
- Related party and vendor personnel are unaware of the entity's confidentiality commitments.
- Confidentiality practices and commitments are changed without the knowledge or consent of internal and external users.