REPORT ON CONFLUENT'S PLATFORM RELEVANT TO SECURITY (SOC 3 REPORT)

FOR THE PERIOD JANUARY 1, 2019 TO DECEMBER 31, 2019

THE cadence GROUP

THE cadence GROUP

O 801.349.1360
F 866.326.6612

PO Box 711190
Salt Lake City, Utah 84171
www.thecadencegroup.com

Section I – Report of Independent Service Auditors

To: Confluent, Inc.

Scope

We have examined Confluent's accompanying assertion, titled "Confluent's Assertion" (assertion), that the controls within Confluent's Platform were effective throughout the period January 1, 2019 to December 31, 2019, to provide reasonable assurance that Confluent's service commitments and system requirements were achieved based on the trust services criteria relevant to security (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

Confluent 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 Confluent's service commitments and system requirements were achieved. Confluent has provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Confluent 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 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 Confluent'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 Confluent's service commitments and system requirements based on the applicable trust services criteria

THE cadence GROUP

O 801.349.1360
F 866.326.6612

PO Box 711190
Salt Lake City, Utah 84171
www.thecadencegroup.com

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

Service Auditor's Independence and Quality Control

We have complied with the independence and other ethical requirements of the Code of Professional Conduct established by the AICPA. We applied the Statements on Quality Control Standards established by the AICPA and, accordingly, maintain a comprehensive system of quality control.

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 are 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 policies or procedures may deteriorate.

Opinion

In our opinion, management's assertion that the controls within Confluent's Platform were effective throughout the period January 1, 2019 to December 31, 2019, to provide reasonable assurance that Confluent's service commitments and system requirements were achieved based on the applicable trust services criteria, is fairly stated, in all material respects.

Cadence Assurance LLC

April 3, 2020
Salt Lake City, Utah

Section II – Confluent's Assertion

We are responsible for designing, implementing, operating, and maintaining effective controls within Confluent's Platform throughout the period January 1, 2019 to December 31, 2019, to provide reasonable assurance that Confluent's service commitments and system requirements relevant to security were achieved.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period January 1, 2019 to December 31, 2019, to provide reasonable assurance that Confluent's service commitments and system requirements were achieved based on the trust services criteria relevant to security (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). Confluent'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.

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, ut 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 January 1, 2019 to December 31, 2019, to provide reasonable assurance that Confluent's service commitments and system requirements were achieved based on the applicable trust services criteria.

Confluent, Inc.
April 3, 2020

Section III – Confluent's Description of its Confluent Service

Company Overview

Confluent was founded by the team that built Apache Kafka. Apache Kafka is a community-distributed, event-streaming platform capable of handling trillions of events a day. Initially conceived as a messaging queue, Kafka is based on an abstraction of a distributed commit log. Since being created and open sourced by LinkedIn in 2011, Kafka has quickly evolved from messaging queue to a full-fledged event streaming platform. Confluent delivers the most complete distribution of Kafka with its Confluent Platform. Confluent Platform improves Kafka with additional community and commercial features designed to enhance the streaming experience of both operators and developers in production, at massive scale. Confluent provides a streaming platform that enables companies to access data as real-time streams. Confluent is headquartered in Mountain View, CA with additional offices in San Francisco, CA and London, UK, and remote workers at various locations. Currently, Confluent employs approximately 1,000 employees across these locations.

Confluent believes every byte of data has a story to tell, something of significance that informs the next thing to be done. In a data-driven enterprise, how data moves is nearly as important as the data itself. With greater speed and agility, data's value increases exponentially.

System Description

The Confluent Platform provides customers with the distribution of Apache Kafka for production environments, simplifying engineering operations and administration of Kafka clusters. It complements Apache Kafka with administration, monitoring, and management tools.

The platform is primarily hosted within a customer's environment and is comprised of the following components:

- *Auto Data Balancer* – Allows organizations and users of the system to:
  - Easily add and remove nodes from Kafka clusters
  - Rebalance partitions across a cluster via rack aware algorithm
  - Throttle traffic from balancing when data transfer occurs
- *Confluent Control Center*™ – A comprehensive management and monitoring system for Apache Kafka. Control Center provides:
  - Users the ability to monitor and manage clusters from a rich user interface
  - Users the ability to quickly scan through clusters for anomalies and track down messages to their sources
  - Full integration with connectors, allowing users to manage data pipelines without a line of code
  - The delivery of real-time analysis of the performance of Kafka
  - The ability to drill into topics, producers, consumers, and more to understand the activity within their data pipelines enabling organizations to govern a growing ecosystem of stream data applications

- *Java Messaging Service (JMS) Client* – An adaptor client, which allows the use of the standard JMS 1.1 Application Programming Interface (API) backed by Kafka. Because the JMS client is a drop-in implementation, it allows users to migrate applications from legacy message queues and gain the modern design, implementation, and scalability of Kafka. Key features allow users to:
  - Develop Java applications leveraging the standard JMS APIs
  - Transparently swap in the JMS client and Kafka without recompiling to migrate applications to Kafka
  - Utilize both producer and consumer APIs
  - Be compatible with most JMS 1.1 features
- *Kafka Connect* – Provides organizations and users with a framework that integrates Kafka with other systems to make it easy to add new systems to scalable and secure stream data pipelines. Connectors translate data between Kafka and other systems, while supporting a variety of data formats and lightweight inline transformations. The following connectors are developed, tested, documented, and fully supported by Confluent Platform:
  - Active MQ Connector (Source)
  - Amazon S3 (Sink)
  - Confluent Replicator (Source & Sink)
  - Elasticsearch (Sink)
  - Filestream Connector (Source & Sink)
  - IBM MQ Connector (Source)
  - HDFS (Sink)
  - JDBC (Source & Sink)
  - JMS (Source)
- *KSQL* – The streaming SQL engine that enables real-time data processing against Apache Kafka. It provides an easy-to-use, yet powerful interactive SQL interface for stream processing on Kafka without the need to write code in a programming language such as Java or Python. KSQL is scalable, elastic, fault-tolerant, and it supports a wide range of streaming operations, including data filtering, transformations, aggregations, joins, windowing, and sessionization.
- *Replicator* – A tool for managing streaming pipelines spanning multiple data centers. It enables users to define topologies spanning multiple data centers and perform multi-datacenter replication to execute these topologies. Replication can be performed in both active/passive and active/active modes between multiple data centers, or to aggregate data into a global data center. Features of Replicator include:
  - Increased reliability by giving users the ability to easily configure and maintain cross-cluster replication and real-time monitoring of replication lag
  - Easy management of multi-cluster deployments
  - Centralized configuration and monitoring
  - The ability to replicate an entire cluster or a subset of topics
  - Automatic replication of topic configuration
  - Automated security using Kafka's Simple Authentication and Security Layer (SASL) for Kerberos and Active Directory

  - Transport Layer Security (TLS) encryption between data centers

- *Security Plugins* – Plugins for other services in Confluent Platform, which add extended security features. Plugins are currently provided for the Representation State Transfer (REST) Proxy and Schema Registry. Key features include principal propagation and pluggable access control. Features of the Security Plugins allow users to:

  - Propagate principles on an incoming REST Proxy request, forwarding them to Kafka
  - Automatically apply Kafka ACLs to REST Proxy requests
  - Propagate principals via TLS and SASL
  - Apply a pluggable authorizer to Schema Registry requests
  - Restrict schema evolution management to administrative users, with read-only access for applications and developers

In addition, the Confluent Platform provides an optional component in Proactive Support. It is included as a plugin for Kafka brokers that proactively reports usage data and metrics to Confluent Support. Metrics metadata is used to provide support and help Confluent improve products. Key features of Proactive Support allow users to:

- Collect and report certain broker and cluster metadata every 24 hours
- Record data to an internal topic in the Kafka cluster and report it via Hypertext Transfer Protocol Secure (HTTPS) to Confluent
- Run in the same Java Virtual Machine (JVM) as the Kafka broker
- Receive an anonymous user report containing a reduced set of usage information
- Report additional operating metrics for customers
- Configure or disable data reporting
- Send reports over an outbound connection from customers' networks to Confluent. Confluent does not have production access to customer environments with this service

For purposes of this report, Confluent systems and networks refer to the Proactive Support component and the underlying infrastructure.

System Boundaries

Included within the scope of this report are the production systems, infrastructure, software, people, procedures, and data supporting Confluent Platform. This report is specific to Confluent Platform and does not include Confluent Cloud.

Subservice Organizations

Confluent utilizes cloud service provider Amazon Web Services (AWS) for Confluent's data center, infrastructure, software, and managed hosting services for the Proactive Support component. AWS is excluded from the scope of this report; the controls for which it is responsible are found in the subsequent section entitled *Complementary Subservice Organization Controls (CSOCs)*.

Principle Service Commitments and System Requirements

Confluent communicates operational requirements to support the achievement of security commitments through its policies and in its contracts with customers. Confluent's commitments are documented and communicated to customers through the following:

- Terms of Service (https://www.confluent.io/marketplace-terms-of-service/)
- Data Processing Addendum (https://www.confluent.io/cloud-customer-dpa/)
- Confluent Security Addendum (https://confluent.io/cloud-enterprise-security-addendum)

System Components

The components of Confluent Platform include the following infrastructure, software, people, procedures, and data elements.

Infrastructure

Confluent Platform is designed, implemented, and operated to achieve specific business objectives in accordance with management-specified requirements. The purpose of the system description is to delineate the boundaries of the system, which include the services outlined above and the components described below.

The primary components of the Confluent Platform are hosted on customer infrastructure, but Confluent utilizes AWS to provide Proactive Support, and to develop, build, and test the other components of the Confluent Platform software for on-premise installations. Proactive Support reports performance metrics back to Confluent over an outbound HTTPS connection and does not provide Confluent personnel access to customer environments.

Software

Confluent has various software programs and tools used to support Confluent Platform. These programs and tools assist with monitoring, authentication, automation of software development, issue tracking, incident response, customer relationship management, and encryption.

People

Confluent teams and functions who support the Confluent environment include Security, Product Engineering, Growth and Marketing, Customer Success, Business Systems, People Operations and Recruiting, Finance, Legal, Information Technology, and Information Security Compliance.

Procedures

Confluent maintains a set of policies that are published and communicated to Confluent personnel. Policies are updated as necessary and are reviewed and approved.

The following policies are relevant to the scope of this report:

- Acceptable Use Policy
- Information Security Policy
- Access Management Standard
- Asset Management Standard
- Business Continuity Plan
- Cloud Security Standard
- Configuration Management Standard
- Cryptography Standard
- Data Classification and Handling Standard
- Incident Management Standard
- Mobile Device Management Standard

- Risk Management Standard
- Vendor Management Standard
- Vulnerability Management Standard

Data

The Confluent Platform is a customer on-premise software package in which the infrastructure is managed by Confluent's customers. As such, Confluent does not process, store, or transmit customer data. Customers are responsible for their own data and infrastructure hosting. The Proactive Support service records and reports metadata about the various operational metrics from the Confluent clusters in the customers' environments to help Confluent improve the overall system. Proactive Support data is transmitted from customer environments to Confluent through an outbound HTTPS connection between Confluent and the customer.

Internal Control Framework

Confluent has adopted the following control framework to meet its security commitments. This framework includes the following aspects: control environment, risk assessment, control activities, information and communication, and monitoring.

Control Environment

An organization's control environment represents the attitude, awareness, and actions of the board of directors, executive management, and other key stakeholders concerning the importance of controls and the emphasis given to controls in the company's policies, procedures, operations, and organizational structure.

Risk Assessment

Confluent maintains an ongoing risk management process intended to proactively identify vulnerabilities within Confluent systems, and assess new and emerging threats to company operations. Processes to assesses and identify risk include risk assessments, vulnerability scans, penetration tests, and an annual review of risk mitigation plans.

Control Activities

Controls have been implemented to address system and data risks. Controls have been designed and implemented in the following areas:

- System inventory
- Physical security
- Perimeter controls
- Network access and logical security
- User access
- Anti-malware protection
- Remote access
- Hardware security
- Vulnerability assessment
- System Monitoring
- Incident management
- Change management
- Backup and disaster recovery

Information and Communication

To help align Confluent's business strategies and goals with operating performance, management is committed to maintaining effective communication both with employees and customers.

External Communications

Contact information for the Customer Success team is available via the company website for customers to make requests, ask questions, and report security incidents or any additional concerns. Customer Success tracks issues to resolution. Customers are specifically notified via email if there are changes to the Terms of Service, Privacy Policy, or Subscriber Agreement.

Internal Communications

Confluent defines job descriptions outlining roles and responsibilities, including those related to designing, developing, implementing, operating, monitoring, and maintaining the Confluent Platform. Job descriptions are made available to enable employee awareness of their responsibilities.

The Security Management Plan and Information Security Policy, which are communicated to internal personnel, define the information security roles and responsibilities. The Security Steering Committee and Head of Information Security approve these documents annually. Employees complete annual security awareness training. Confluent publishes written policies and procedures to its employees related to the following areas: acceptable use, access management, asset management, cloud security, configuration management, cryptography standard, data classification and handling, mobile device management standard, incident management, information security, risk management, vendor management, and vulnerability management.

Monitoring

Confluent has developed a suite of controls to monitor the compliance of its control environment. These controls are designed to be complimentary to Confluent's existing suite of controls. Monitoring control activities include annual vendor assessments and an annual internal control evaluation.

Complementary User Entity Controls

Confluent's controls were designed under the assumption that certain controls would be implemented by user organizations, the application of which is necessary to meet certain trust services criteria identified in this report. This section highlights those internal control responsibilities Confluent believes should be present at each customer, and has considered in developing its controls reported herein. Confluent customers should evaluate their own control environment to assess if the following controls are implemented and operating effectively. These complementary user entity controls do not represent a comprehensive list of controls that should be employed by Confluent customers, but provide a summary of controls necessary to meet the stated trust services criteria presented in this report. These controls include the following:

- User entities are responsible for provisioning, deprovisioning and reviewing user access, including Confluent Customer Support personnel within the Confluent Platform (CC6.1, CC6.2, CC6.3).
- User entities are responsible for ensuring infrastructure systems used to support the Confluent Platform are appropriately secured (CC6.1, CC6.2, CC6.3, CC6.6).
- User entities are responsible for sending data to Confluent via a secure connection designated by Confluent and/or the data should be encrypted (CC6.7).
- User entities are responsible for evaluating Confluent Platform software package updates against the user entities' internal security and functional requirements prior to implementing within their environments (CC8.1).
- User entities are responsible for testing Confluent Platform software package updates for any client-specific needs and appropriately implementing these updates within their environments (CC8.1).

Complementary Subservice Organization Controls

Confluent contracts with Amazon Web Services (AWS) to provide data center, infrastructure, software, and managed hosting services. Controls managed by the third-party subservice provider are not included in the scope of this report. Expected subservice provider controls that have an effect on specific criteria are included below.

Criteria	Expected Controls
CC6.1 – The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	Access to hosted systems requires users to use a secure method to authenticate. User content is segregated and made viewable only to authorized individuals. Network security mechanisms restrict external access to the production environment.
CC6.2 – Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	New user accounts are approved by appropriate individuals prior to being provisioned. User accounts are removed when access is no longer needed. User accounts are reviewed on a regular basis by appropriate personnel.
CC6.3 – The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.	Access modifications to hosted systems are approved by appropriate individuals prior to being provisioned. User accounts are removed when access is no longer needed. User accounts are reviewed on a regular basis by appropriate personnel.
CC6.4 – The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	Access to physical facilities is restricted to authorized users.
CC6.5 – The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.	Production media is securely decommissioned and physically destroyed prior to being removed from the data center.

Criteria	Expected Controls
CC6.6 – The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	Network security mechanisms restrict external access to the production environment. Encrypted communication is required for connections to the production system.
CC6.7 – The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.	Access to hosted data is restricted to appropriate users. Hosted data is protected during transmission through encryption and secure protocols.
CC6.8 – The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.	Antivirus or antimalware solutions are installed to detect or prevent unauthorized or malicious software.
CC7.1 – To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.	System configurations changes are logged and monitored. Vulnerabilities are identified and tracked to resolution.
CC7.2 – The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	Security events are monitored and evaluated to determine potential impact per policy.
CC7.3 – The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.	Operations personnel log, monitor and evaluate to incident events identified by monitoring systems
CC7.4 – The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	Operations personnel respond, contain and remediate incident events, and update stakeholders, as needed.
CC8.1 – The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	System changes are documented, tested, and approved prior to migration into production. Access to make system changes is restricted to appropriate personnel.