REPORT ON CONFLUENT’S PLATFORM RELEVANT TO SECURITY AND CONFIDENTIALITY (SOC 3 REPORT)

FOR THE PERIOD JANUARY 1, 2020 TO DECEMBER 31, 2020
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, 2020 to December 31, 2020, to provide reasonable assurance that Confluent’s service commitments and system requirements were achieved based on the trust services criteria relevant to security 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
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
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 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, 2020 to December 31, 2020, 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**

March 26, 2021
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, 2020 to December 31, 2020, to provide reasonable assurance that Confluent’s service commitments and system requirements relevant to security and confidentiality were achieved. Our description of the boundaries of the system is presented in Attachment 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 January 1, 2020 to December 31, 2020, to provide reasonable assurance that Confluent’s service commitments and system requirements were achieved based on the trust services criteria relevant to security 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). 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. The principal service commitments and system requirements related to the applicable trust services criteria are presented in Attachment 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 January 1, 2020 to December 31, 2020, to provide reasonable assurance that Confluent’s service commitments and system requirements were achieved based on the applicable trust services criteria.

Confluent, Inc.
March 26, 2021
Attachment A – Confluent’s Description of the Boundaries of its Confluent Platform

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 a messaging queue to a full-fledged event streaming platform. Confluent delivers the most complete distribution of Kafka with its Confluent Platform. The 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, Austin, TX, and London, UK, and remote workers at various locations. Currently, Confluent employs approximately 1,300 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
Confluent Platform provides customers with the distribution of Apache Kafka for production environments simplifying engineering operations and the administration of Kafka clusters. It complements Apache Kafka with administration, monitoring, and management tools. The Confluent Platform is primarily hosted within a customer’s environment and is comprised of the following components:

- **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

- **Confluent Operator** – Confluent Operator allows users to deploy and manage Confluent Platform as a cloud-native, stateful container application on Kubernetes and OpenShift. The automation provided by Kubernetes, Operator, and Helm greatly simplifies provisioning and
minimizes the burden of operating and managing Confluent Platform clusters. Operator also provides users with the portability to use Apache Kafka® in multiple provider zones and across both private and public cloud environments.

- **Kafka Connect** – A tool for scalability and reliably streaming data between Apache Kafka® and other data systems. It makes it simple to quickly define connectors that move large data sets into and out of Kafka. Kafka Connect can ingest entire databases or collect metrics from application servers into Kafka topics, making the data available for stream processing with low latency. An export connector can deliver data from Kafka topics into secondary indexes like Elasticsearch or into batch systems such as Hadoop for offline analysis. Available connectors may be installed separately via Confluent Hub.

- **ksqlDB** – ksqlDB is the streaming SQL engine for 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. ksqlDB is scalable, elastic, fault-tolerant, and real-time. It supports a wide range of streaming operations, including data filtering, transformations, aggregations, joins, windowing, and sessionization.

- **Proactive Support** – An optional plugin for Kafka brokers that proactively reports usage data and metrics to Global Technical Support. Metrics metadata is used to provide proactive support and help Confluent improve products. Key features of Proactive Support include:
  - The collection and reporting of certain broker and cluster metadata every 24 hours
  - The recording of data by default to an internal topic in the Kafka cluster and reports via HTTPS to Confluent
  - The execution of the program in the same Java virtual machine as the Kafka broker
  - The reporting of minimal usage information by anonymous users
  - The reporting of additional operating metrics for customers
  - The ability to configure and disable data reporting
  - The distribution of reports over an outbound connection from customers’ networks to Confluent (and Confluent does not have production access to customer environments with this service)

- **Replicator** – Confluent Replicator can be deployed across clusters and in multiple data centers. Multi-data center deployments enable use cases, such as:
  - Active-active geo-localized deployments – allows users to access a near-by data center to optimize their architecture for low latency and high performance
  - Active-passive disaster recovery (DR) deployments – allows the failing over applications to use Confluent Platform in a different data center if a disaster occurs
  - Centralized analytics – Aggregates data from multiple Apache Kafka® clusters into one location for organization-wide analytics
  - Cloud migration – Uses Kafka to synchronize data between on-prem applications and cloud deployments

- **Schema Registry** – The Confluent Schema Registry provides a serving layer for metadata. Specifically, it provides a RESTful interface for storing and retrieving Avro®, JSON Schema, and
Protobuf schemas. It stores a versioned history of schemas based on a specified subject name strategy, provides multiple compatibility settings and allows evolution of schemas according to the configured compatibility settings and expanded support for these schema types. It also provides serializers that plug into Apache Kafka® clients to handle schema storage and retrieval for Kafka messages sent in any of the supported formats.

- **Security Plugins** – Plugins for other services in the Confluent Platform which add extended security features. Plugins are currently provided for the Representational 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 principals on an incoming REST Proxy request, forwarding them to Kafka
  - Automatically apply Kafka ACLs to REST Proxy requests
  - Propagate principals via SSL 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.

- **Self-Balancing Clusters** – Self-Balancing automates resource workload balancing, provides failure detection and self-healing, and allows adding or decommissioning brokers as needed, with no manual tuning required. Self-balancing provides:
  - Fully automated load balancing
  - Auto-monitoring of clusters for imbalances based on a large set of parameters, configurations, and runtime variables
  - Continuous metrics aggregation and rebalancing plans, generated instantaneously in most cases, and executed automatically
  - Automatic triggering of rebalance operations based on simple configurations set on Confluent Control Center or in Kafka server properties files (Users can choose to auto-balance only when brokers are added, or anytime, which rebalances for any uneven load.)
  - At-a-glance visibility into the state of the clusters and the strategy and progress of auto-balancing through a few key metrics.

**System Boundaries**

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

**Subservice Organizations**

Confluent utilizes cloud service provider Amazon Web Services (AWS) for Confluent’s data center, infrastructure, software, and hosting services for the Proactive Support component. AWS is excluded from the scope of this report; the controls it is expected to provide are included in Attachment D, titled *Complementary Subservice Organization Controls (CSOC)*.


System Components

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

Infrastructure

The 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.

Infrastructure for the Confluent Platform is unique and delimited. 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-premises 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 the 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 Business Systems, Global Technical Support, Engineering, Finance, Growth and Marketing, Information Technology, Legal, Security Steering Committee, People Operations and Recruiting, and Product.

Procedures

Confluent has developed and communicated to its personnel procedures to protect service data and the company’s assets. Teams are expected to adhere to Confluent policies and procedures that define data is protected through rules and requirements. These are located on the company’s Intranet and shared drive and can be accessed by any Confluent employee.

The policies and standards used to safeguard Confluent Platform include:

- Acceptable Use Policy
- Access Management Standard
- Asset Management Standard
- Business Continuity and Disaster Recovery Plan
- Configuration Management Standard
• Cryptography Standard
• Data Classification and Handling Standard
• Information Security Policy
• Logging and Monitoring Standard
• Mobile Device Management Standard
• Risk Management Standard
• Security Incident Response Standard
• Vendor Management Standard
• Vulnerability Management Standard

Data

Confluent Platform is a customer on-premises 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 and confidentiality commitments. This framework includes the following aspects: control environment, risk assessment, control activities, information and communication, and monitoring.

Additionally, complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Confluent, to achieve Confluent’s service commitments and system requirements based on the applicable trust services criteria. See Attachment C for identified complementary user entity controls.

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. Management has implemented the necessary governance to establish this tone. Specifically, Confluent has implemented management meetings, an organizational structure, policies, and practices to establish an effective tone.

Risk Assessment

Confluent maintains an ongoing risk management process to proactively identify, evaluate and manage risks and vulnerabilities within Confluent systems, and to assess new and emerging threats to company operations. Processes to identify, evaluate, and mitigate these risks include risk assessments, vulnerability scans, penetration tests, vendor risk assessments, 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
- Logical access
- Corporate network
- User provisioning and deprovisioning
- Access reviews
- Anti-malware protection
- Encryption
- Data management
- Vulnerability assessment
- System monitoring
- Incident management
- Change management
- Configuration 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

Descriptions of Confluent Platform and its boundaries are available to external users. Contact information for the Global Technical Support team is available via the company website for customers to make requests, ask questions, and report security incidents or any additional concerns. The Global Technical Support team tracks and resolves customer-reported incidents via the customer ticketing system. Significant changes to application functionality are communicated to customers via release notes after the implementation of the change.

Internal Communications

Confluent defines job descriptions outlining roles and responsibilities, including those related to designing, developing, implementing, operating, monitoring, and maintaining the Confluent systems. 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, 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 complementary to Confluent’s existing suite of controls. Monitoring control activities include, annual vendor assessments, and an annual internal control evaluation.
Attachment B – Principal Service Commitments and System Requirements

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

- System Requirements ([https://docs.confluent.io/installation/system-requirements.html](https://docs.confluent.io/installation/system-requirements.html))

Confluent has adopted a control framework to meet its commitments. This framework includes the following aspects: control environment, risk assessment, control activities, information and communication, and monitoring outlined in Attachment A.
Attachment C – 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).
Confluent contracts with 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 trust services criteria include the following:

- Access to hosted systems requires strong authentication mechanisms (CC6.1).
- Data at rest on hosted systems is stored in an encrypted format (CC6.1).
- New and existing user access and permissions to hosted systems are approved by appropriate personnel prior to being granted (CC6.1, CC6.2, CC6.3).
- Terminated user access permissions to hosted systems are removed in a timely manner (CC6.1, CC6.2, CC6.3).
- User access permissions to hosted systems are reviewed by appropriate personnel on a regular basis (CC6.2, CC6.3).
- Privileged access to hosted systems and the underlying data is restricted to appropriate users (CC6.3, CC6.7).
- Access to the physical facilities housing hosted systems is restricted to authorized users (CC6.4).
- Production media is securely decommissioned and physically destroyed prior to being removed from the data center (CC6.5).
- Network security mechanisms restrict external access to the production environment to authorized ports and protocols (CC6.6).
- Connections to the production environment require encrypted communications (CC6.6, CC6.7).
- Anti-virus or anti-malware solutions detect or prevent unauthorized or malicious software on hosted systems (CC6.8).
- System configuration changes are enforced, logged, and monitored (CC6.8, CC7.1).
- Hosted systems are scanned for vulnerabilities. Any identified vulnerabilities are tracked to resolution (CC7.1).
- System activities on hosted systems are logged, monitored and evaluated for security events. Any identified incidents are contained, remediated and communicated according to defined protocols (CC7.2, CC7.3, CC7.4).
- Access to make changes to hosted systems is restricted to appropriate personnel (CC8.1).
- Changes to hosted systems are documented, tested, and approved prior to migration to production (CC8.1).