petersonsullivan LLP

Certified Public Accountants
& Advisors

Cloudflare

Global Cloud Platform

For Enterprise Customers

System and Organization Controls 3 (SOC 3) Report
Relevant to Security, Availability and Confidentiality
For the period May 01, 2019 to October 31, 2019

Table of Contents

Section I

Independent Service Auditor's Report

petersonsullivan LLP
Certified Public Accountants
& Advisors

INDEPENDENT SERVICE AUDITOR'S REPORT

To the Management of Cloudflare, Inc.
San Francisco, California

Scope

We have examined management's assertion titled "Management's Assertion" (assertion) that the controls within Cloudflare's Global Cloud Platform (system) were effective throughout the period May 01, 2019 to October 31, 2019, to provide reasonable assurance that Cloudflare'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

Cloudflare 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 Cloudflare's service commitments and system requirements were achieved. Cloudflare has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Cloudflare 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 and 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.

601 Union Street
Suite 2300
Seattle, WA 98101

(206) 382-7777 MAIN
(206) 382-7700 FAX

pscpa.com

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 Cloudflare'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 Cloudflare'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.

Our examination was not conducted for the purpose of evaluating Cloudflare's cybersecurity risk management program. Accordingly, we do not express an opinion or any other form of assurance on its cybersecurity risk management program.

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 Cloudflare's Global Cloud Platform were effective throughout the period May 01, 2019 to October 31, 2019, to provide reasonable assurance that Cloudflare's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

Peterson Sullivan LLP

Peterson Sullivan LLP
December 19, 2019

Section II
Management's Assertion

MANAGEMENT'S ASSERTION

We are responsible for designing, implementing and maintaining effective controls over the system titled Cloudflare's Global Cloud Platform (System) throughout the period May 01, 2019 to October 31, 2019, to provide reasonable assurance that Cloudflare'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 III and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls over the system throughout the period May 01, 2019 to October 31, 2019, to provide reasonable assurance that Cloudflare'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). Cloudflare'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 principle service commitments and system requirements related to the applicable trust services criteria are presented in Section III.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of 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 May 01, 2019 to October 31, 2019, to provide reasonable assurance that Cloudflare's service commitments and system requirements were achieved based on the applicable trust services criteria.

Cloudflare Management
December 19, 2019

Section III

Description of System Boundaries, Principal Service Commitments and System Requirements

Provided by Cloudflare

COMPANY OVERVIEW AND BACKGROUND

Cloudflare, Inc. (Cloudflare) was founded in 2009 with the core mission of helping to build a better Internet. Cloudflare is a cloud-based company that provides security, performance and reliability services, such as a Content Delivery Network (CDN) solution, distributed denial-of-service (DDoS) mitigation, Domain Name System (DNS), Web Application Firewall (WAF), and more that are included with Cloudflare's Enterprise plan. Cloudflare also provides Enterprise customers paid enhancements that customers can utilize to increase the level of their website's security, performance, and reliability. Cloudflare's technology is hosted on cloud computing infrastructure and the product dashboard can be accessed from any web browser.

OVERVIEW OF PRODUCTS AND SERVICE COMMITMENTS

Cloudflare provides products to the public-facing internet through their Global Cloud Platform. Cloudflare's Global Cloud Platform includes the Cloudflare Edge, the Cloudflare Dashboard, and core platform management components.

The Cloudflare Edge is a cloud scale global infrastructure of points of presence (PoPs) that are located in globally distributed colocations that span 194 cities in 90 countries as of October 31, 2019. Each PoP contains managed devices, internally known as "metals." The metals host servers which have proprietary operating system designs to delineate how certain traffic should be handled and managed (deliver Cloudflare products). All Edge metals are identical in design and centrally managed the same way, through a data center management (DM) node. Cloudflare's network of Edge PoPs is designed to be resilient and fault tolerant to help maintain the confidentiality, integrity, and availability of Cloudflare customer sensitive data. A full map of Cloudflare's globally distributed colocations is available, at (https://www.Cloudflare.com/network/).

Customers interact with the Cloudflare products through the Cloudflare dashboard hosted at https://dash.Cloudflare.com/. Enterprise customers that use the Cloudflare products receive several security, performance and reliability enhancements services, such as a CDN solution, DDoS mitigation, DNS, and WAF. In addition to these base products, there are also more paid enhancements that customers can utilize to increase the level of their website's security, performance, and reliability. The dashboard provides client program administrators the ability to enable functionality, and the portal provides insights into analytics, logs of account changes, service updates, and the ability to set client configurations.

Cloudflare's core platform management components are located in Cloudflare's primary colocation facilities in Portland, Oregon; San Francisco, California; San Jose, California; Seattle, Washington; and Luxembourg.

The major products served through the Cloudflare Global Cloud Platform are:

Products	**Details:**
Performance and Reliability ● CDN ● DNS ● Argo Smart Routing ● Load Balancing ● Web Optimization	● **CDN** provides faster web page load times by serving content from locations closer to the user. ● Cloudflare **DNS** is DDoS protection for domain resolution. DNS comes with built-in load-balancing, automatic failover, rate-limiting, and filtering. ● **Argo Smart Routing** leverages real-time network intelligence to route traffic across the fastest, most reliable paths from the origin to a Cloudflare Edge PoP. ● **Load Balancing** is Cloudflare's cloud solution to balancing local and global traffic across multiple servers or by routing traffic to the closest geolocation region. ● **Web Optimization** products include: local storage caching, rocket loader, and accelerated mobile links.
Advanced Security ● DDos Protection ● WAF ● Rate Limiting ● SSL/TLS ● DNSSEC ● Cloudflare Access ● Cloudflare Spectrum ● Argo Tunnel ● Magic Transit	● **DDos** mitigation to maintain performance and availability. Includes IP reputation database and high network capacity. ● **WAF** is our web application firewall that analyzes request parameters to detect and block common application layer vulnerabilities at the network edge. ● **Rate Limiting** allows customers to easily set up rules that restrict the number of requests that hit their origin servers from the same IP address. ● **SSL/TLS** is the standard security technology for establishing an encrypted link between a web server and a browser. Cloudflare offers multiple options for SSL/TLS to ensure that visitors are always accessing a customer website over a secure HTTPS connection. ● **DNSSEC:** If DNS is the phone book of the Internet, DNSSEC is the Internet's unspoofable caller ID. It guarantees a web application's traffic is safely routed to the

	correct servers so that a site's visitors are not intercepted by a hidden "man-in-the-middle" attacker. ● **Cloudflare Access:** Secure Application Access Without a VPN. Secure, authenticate, and monitor user access to any domain, application, or path on Cloudflare. ● **Cloudflare Spectrum** provides the power of Cloudflare's DDoS, TLS, and IP Firewall to not just web-servers, but also other TCP-based products running on a customer's origin servers. ● **Argo Tunnel:** Cloudflare's lightweight Argo Tunnel daemon creates an encrypted tunnel between your origin web server and Cloudflare's nearest Edge PoP — all without opening any public inbound ports. ● **Magic Transit:** Cloudflare's software-defined networking product that offers IP transit with DDoS protection, next-gen firewall, traffic acceleration and more for your on-premise and data center networks from a single, easy-to-use interface.
Insights ● Analytics	● Analytics delivers and demonstrates Cloudflare value to customers through actionable data straight from the Cloudflare Dashboard. Cloudflare Enterprise customers have access to raw logs of HTTP requests for their domains. These logs are helpful for debugging, identifying configuration adjustments, and creating analytics, especially when combined with other data sources, such as application server logs.

SCOPE AND SYSTEM BOUNDARIES

The scope of this description covers the Cloudflare Global Cloud Platform through which Cloudflare provides security, reliability and performance products to Enterprise customers, and excludes other products provided by Cloudflare. The description does not encompass every aspect of all the products provided or procedures followed by Cloudflare. Rather, the description enables current user entities and future user entities to understand how controls in place for the Global Cloud Platform are critical to Cloudflare's business and the overall control environment.

This description does not include Cloudflare's China-based platform and products served through Cloudflare's China-based platform.

Cloudflare uses subservice organizations to provide data center colocation and hosting services. The description includes only the controls of Cloudflare and excludes the controls at the subservice organizations as delineated below in Section III, Complementary Subservice Organization Controls.

COMPONENTS OF THE CLOUDFLARE GLOBAL CLOUD PLATFORM AND SYSTEM REQUIREMENTS

The purpose of the Global Cloud Platform for Enterprise customers description is to delineate the boundaries of the Global Cloud Platform, which includes the products listed above and the four components described below: infrastructure (primary and logical architecture), software, personnel, and procedures.

Infrastructure

The Global Cloud Platform includes the following infrastructure elements:

Primary Infrastructure			
Hardware	**Location**	**Type**	**Purpose**
Routers, Switches, Servers, Firewalls	Portland (PDX)	Compute, Primary Data Warehouse, Security, Cloud	Provides fault tolerant servers for the clusters, open source streaming software servers, open source DBMS for real-time generation of analytical reports, applications with API's for resource management and scheduling across the cloud environment and speeds searches for analytics.
	San Francisco (SFO)	Development Environment	Provides staging and pre-production environment for major products and services provided on the Edge.
	Luxembourg (LUX)	Secondary Data Warehouse	Provides redundancy and recovery capabilities for the primary data warehouse.
	Intermediary Edge PoPs (SJC and SEA)	Core Services	Intermediary Edge PoPs that serve major products to the Global Edge Network from PDX.

Primary Infrastructure			
Hardware	**Location**	**Type**	**Purpose**
	Global Edge PoPs	Core Services	Edge PoPs that deliver Cloudflare products to the public internet

Software

Primary Software	
Software	**Purpose**
User Provisioning Software ● Cloud-based business productivity tools ● Internal project management & developer tools ● Password manager ● VPN client	● Used for communication and file storage ● Planning, tracking, and executing projects, as well as for internal documentation ● For generating strong credentials and storing them securely ● Support remote VPN connection from endpoints
Operations Software ● Encryption software ● Organization chart software ● Endpoint security software ● Learning Management System ● Recruiting software service ● E-signature service ● Customer support dashboard ● Bug bounty service ● Customer Relationship Management (CRM) service	● Disk and file encryption software. ● Live organization chart and directory. ● Anti-malware and anti-virus. ● Scalable employee training deployment and management. ● Job posting, job application management, and interview process handling ● Authenticating and managing electronic agreements ● Vulnerability management platform for connecting with security researchers and establishing guidelines for reporting security findings on our services ● Service for enterprise customer

	account management
Monitoring Software	• Corporate and production network monitoring, alerting and prevention tool • Alerting service • Automatic attack handling pipeline tool • Aggregation dashboard providing insight into detected attacks
Source Code Management Software	• Internal hosting application for version control of production and application source code • Configuration management software and remote execution engine • Build server application for continuous integration
Databases	• Master PostgreSQL database that holds most of the customer information for Cloudflare.

Personnel

Cloudflare utilizes the following functional areas of operations to support the Cloudflare Global Cloud Platform within the scope of this review:

- Cloudflare Board of Directors - Responsible for making objective evaluations and decisions regarding the Company's mission, vision, and values.
- Cloudflare Security Steering Committee - At Cloudflare, the role of the Security Steering Committee is to coordinate corporate security initiatives at the executive level and thus enable Cloudflare to optimize spending, allocate resources, provide oversight, and minimize security risk.
- Engineering - Responsible for the development and delivery of Cloudflare's internal tools and Global Cloud Platform. The engineering team is also comprised of site reliability engineers who are responsible for maintenance and monitoring the availability and capacity of the Global Cloud Platform.
- Technical Operations - Responsible for maintaining operational stability across Cloudflare's Global Cloud Platform.
- Customer Support - Responsible for solving customer problems, issues, and incidents.
- Security - Responsible for direct input into the development and implementation of information security, availability and confidentiality requirements. Security is comprised of the Security Compliance team, responsible for the oversight of all security compliance requirements and Product Security, who is responsible for maintaining and developing secure products.
- HR/People Team - Responsible for the recruiting and development of Cloudflare employees. Responsibilities include, but not limited to, maintaining organizational structure, onboarding employees, and offboarding employees.
- Legal - Responsible for creating systems and policies that support Cloudflare's Global Cloud Platform including, among other things, customer contracts, confidentiality agreements, and internal communication channels. The Data Protection Officer is also a member of the Legal team and is responsible for the legal oversight of data privacy.
- Infrastructure - Responsible for building, monitoring, and maintaining the global network of Edge PoPs for Cloudflare.
- IT - Responsible for the administration and maintenance of internal Cloudflare systems including providing and revoking system access to employees.

Policies and Procedures

Cloudflare has put into place a set of policies and procedures to help ensure that security commitments are met. Cloudflare has established information security policies and procedures to address commitments to security, availability, and confidentiality of customer data. The policies and procedures are updated and reviewed annually, and the current policies and procedures are available on Cloudflare's intranet. Management has identified actions, in the form of control activities, and put these into place to enforce the management defined standards. In addition, Cloudflare has documented and made available on their website security related documents that describe user accessibility, security features, and methods for user interaction.

Data

As stated in the Privacy Policy, Cloudflare processes three types of data with respect to their customers: (1) Cloudflare stores information related to a customer's account (e.g., name, email address, payment information); (2) Cloudflare transmits customers' web content through our edge servers as a reverse proxy, and may store limited static content in our edge servers if a customer is utilizing our CDN Services; and (3) Cloudflare processes web traffic information on behalf of our customers.

Our customers control how long we store cached data while their accounts are active, and that data is deleted from our servers when an account is deleted. Additionally, our customers have the ability to purge data from the cache at any time.

Overview of System Incidents

On July 2, 2019 Cloudflare deployed a new rule in the WAF Managed Rules that caused CPUs to become exhausted on every CPU core that handles HTTP/HTTPS traffic on the Cloudflare network worldwide. The July 2nd update contained a regular expression that backtracked enormously and exhausted CPU used for HTTP/HTTPS serving which brought down Cloudflare's core proxying, CDN and WAF functionality for 27 minutes. For more detail please visit our blog post (accessible here: https://blog.cloudflare.com/details-of-the-cloudflare-outage-on-july-2-2019/) on the incident.