Introduction and scope

As companies increasingly evaluate the security posture of vendors they intend to buy services from, the importance of security compliance certifications grows. Security compliance certifications are reports created by independent, third-party auditors that validate and document a company's commitment to security. These external auditors will conduct a rigorous review of a company's technical environment and evaluate whether or not there are thorough controls—or safeguards—in place to protect the security, confidentiality, and availability of information stored and processed in the environment.

SOC 2 was established by the American Institute of CPAs. It consists of a technical audit and a requirement that comprehensive information security policies and procedures be written and followed. Cloudflare obtained our SOC 2 validation in 2019, and includes the report as part of our compliance package for current and potential customers under NDA. The more general, public version of the SOC 2 report is the SOC 3. It can be downloaded from our website here. In addition, aA detailed overview of our security compliance journey can be found here.

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.

Frequently asked questions about Cloudflare and SOC 2

What accounts are in-scope for Cloudflare's SOC 2 report?
Enterprise customers are in-scope for Cloudflare's SOC 2 report

How do customers get a copy of the SOC 2 Report?
Customers can request a copy of Cloudflare's SOC 2 report by contacting their Account Executive. Cloudflare requires all customers to sign a nondisclosure agreement before our report is provided.

What Trust Service Criteria are in-scope for SOC 2?
Cloudflare's SOC 2 scope currently covers the security, confidentiality, and availability trust service criteria.

What Cloudflare products are not in-scope for SOC 2?
This description does not include Cloudflare's China-based platform and products served through Cloudflare's China-based platform. In addition, the following Cloudflare products are not in-scope for SOC 2:

- Baidu
- Magic Transit
- Stream

What are the SOC 2 User Entity Controls?

Users should consider whether the following controls have been placed in operation at user organizations:

User entities of Cloudflare's system are responsible for:	**Applicable Trust Services Criteria**
Establishing strong passwords and maintaining the confidentiality of Authorized users' usernames and password.	CC5.1, CC5.2, CC6.1, CC6.6
Enabling two-factor authentication in conjunction with usernames and passwords.	CC5.1, CC5.2, CC6.1, CC6.6
Acknowledging and agreeing that only Authorized Users are entitled to access the Service with their assigned usernames and passwords provided by Cloudflare.	CC2.3, CC6.1, CC6.2, CC6.3, CC6.5
Notifying Cloudflare promptly of any actual or suspected unauthorized use of any Authorized User's account, username, or password, or any other breach or suspected breach of the Agreement.	CC2.3, CC4.2, CC7.1, CC7.3, CC7.4, CC7.5
Supporting and maintaining the availability of its website(s), the connectivity of its website(s) to the Internet, and all Customer Content, IP addresses, domain names, hyperlinks, databases, applications and other resources as necessary for Customer to operate and maintain its website(s) to meet Customer's business requirements and to utilize the service.	CC2.3, A1.1, A1.2
Keeping and maintaining own copy of all Customer Log Files, once delivered to Customer.	CC5.1, CC5.2, A1.1, A1.2

Knowing what data they want and need to have cached.	CC9.1, CC8.1, CC6.7, A1.1, A1.2
Agreeing and allowing Cloudflare to act as its limited agent pursuant to the terms and conditions of the Agreement, for the purpose of providing Internet data and optimization services.	CC1.1
Complying with all laws applicable to its purchase and use of the Service, including without limitation, the export and import regulations of other countries.	CC3.1, CC1.1

Using available features or services, agreeing and acknowledging that Customer may be required to accept the licenses or agreements associated with such features or services, and to install additional software modules to use such features or services.	CC2.3, CC8.1
Updating its information with Cloudflare, including providing Cloudflare with an up-to-date e-mail address for the provisioning of notices under the Agreement.	CC2.3, CC8.1
Not assigning, subcontracting, delegating, or otherwise transferring the Agreement or its rights and obligations herein, in whole or in part, by operation of law or otherwise, without obtaining the prior written consent of Cloudflare.	CC1.1, CC2.3, CC8.1
Representing and warranting that the information it provides to Cloudflare regarding its network usage (including but not limited to bandwidth usage, number of domains, geographic location of users, and SSL requirements) in order to obtain a price quote which forms the basis of the Agreement, is truthful, accurate, and complete, to the best of its knowledge.	CC1.1, CC2.3, CC8.1
Complying with the Enterprise Subscription Terms of Service and agreeing not to use the Service in connection with any: (a) infringement or misappropriation of any Intellectual Property Rights; (b) defamation, libel, slander, obscenity, or violation of the rights of privacy or publicity of any person or entity; or (c) other offensive, harassing, or illegal conduct.	