1Password

Achieving SOC 2 compliance with 1Password



SOC 2 is a compliance framework that ensures service providers securely manage data to protect the privacy and interests of their clients. Maintaining SOC 2 compliance can be challenging as organizations manage growing SaaS, identity, and device environments in a hybrid environment. 1Password helps organizations meet these requirements by enforcing strong security policies, protecting every identity and endpoint, and simplifying audit readiness. With integrations with Drata, 1Password strengthens governance and makes it easier for customers to maintain ongoing SOC 2 adherence for their compliance requirements.

Disclaimer: This document describes how 1Password capabilities may be used to support an organization's implementation of select the 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus – 2022) established by the AICPA's Assurance Services Executive Committee (ASEC).The information provided is intended for informational purposes only and does not constitute legal, regulatory, or compliance advice.

Customers are responsible for establishing and maintaining the policies, procedures, and governance controls necessary to meet SOC 2 requirements. Implementation of 1Password products alone does not guarantee compliance.

SOC 2 Requirement ID

CC3.2.4

Requirement description

Estimates Significance of Risks Identified — Identified risks are analyzed through a process that includes estimating the potential significance of the risk.

How 1Password products/features can support SOC 2 compliance

1Password Enterprise Password Manager: Business Watchtower provides organizations with visibility into password hygiene and security risks, including identifying weak, reused, or compromised passwords and highlighting applications and websites where users can enable two-factor authentication.

1Password Device Trust: Device Trust helps organizations with continuous monitoring of organizational systems and applications by providing administrators with OSQuery-based tools to perform live queries on endpoint devices. Admins can continuously monitor system configurations and software versions to detect potential vulnerabilities allowing for immediate assessment and response.

1Password SaaS Manager: 1Password SaaS Manager provides visibility into organization's SaaS ecosystem and the continuous discovery of new applications (including identification of shadow IT) and insights into user access.

Additional resources

Use Watchtower to find account details you need to change

Total Fleet Visibility with Device Trust

SOC 2 Requirement ID

CC3.2.5

Requirement description

Determines How to Respond to Risks—Risk assessment includes considering how the risk should be managed and whether to accept, avoid, reduce, or share the risk.

How 1Password products/features can support SOC 2 compliance

1Password Enterprise Password Manager: Business Watchtower provides ongoing insight into the security health and maturity of your tenant. 1Password Watchtower integrates with Have I Been Pwned and will alert if any of your passwords have appeared in data breaches. It also flags weak or duplicate passwords, and websites where users can turn on two-factor authentication.

1Password Device Trust: Device Trust helps organizations with continuous monitoring of organizational systems and applications by providing administrators with OSQuery-based tools to perform live queries on endpoint devices. Admins can continuously monitor system configurations and software versions to detect potential vulnerabilities allowing for immediate assessment and response.

1Password SaaS Manager: 1Password SaaS Manager provides visibility into organization's SaaS ecosystem and the continuous discovery of new applications (including identification of shadow IT) and insights into user access.

Additional resources

Use Watchtower to find account details you need to change

Device Trust Live Query

SOC 2 Requirement ID

CC5.2.3

Requirement description

Establishes Relevant Security Management Process Controls Activities—Management selects and develops control activities that are designed and implemented to restrict technology access rights to authorized users commensurate with their job responsibilities and to protect the entity's assets from external threats.

How 1Password products/features can support SOC 2 compliance

1Password Enterprise Password Manager: Supports access management through custom groups, allowing administrators to define granular permissions that govern how users and groups interact with the tenant and its controlled content. The 1Password automated provisioning integrations enhances this by integrating with an organization's identity provider (IdP), facilitating automated and scalable user provisioning and access management.

1Password SaaS Manager: Provides features that can help organizations provision and manage user access to their applications with ability to record the how and when access was granted, including approvals from system owners and the specific level of access granted. Organizations can further configure access parameters for each application, with customizable access policies that simplify the process of granting access to tools based on teams or roles.

Additional resources

Use custom groups in 1Password Enterprise Password Manager

Manage Access to Apps

SOC 2 Requirement ID

CC6.1.1

Requirement description

Identifies and Manages the Inventory of Information Assets—The entity identifies, inventories, classifies, and manages information assets.

How 1Password products/features can support SOC 2 compliance

1Password Device Trust: Provides fleet visibility across MAC, Windows and Linux endpoints. Once enabled on the user endpoint; Device Trust provides administrators with detailed insight into that state of devices and runs checks on devices to ensure that meet organization's security and compliance requirements.

1Password SaaS Manager: Device register allows organizations to manage devices like laptops, computer displays, and network equipment. It tracks each device's status, location, and assigned user, while also giving administrators the ability to set up automated workflows for device reconditioning and replacement. The device register can be populated by connecting to an external system or by importing/adding details manually. Additionally 1Password SaaS Manager also provides continuous discovery of new applications and unmanaged applications being used across the organization allowing for insights into shadow IT.

Additional resources

Manage devices in SaaS Manager

Device Trust Fleet Visibility

SOC 2 Requirement ID

CC6.1.3

Requirement description

Restricts Logical Access—The entity restricts logical access to information assets, including infrastructure (for example, server, storage, network elements, APIs, and endpoint devices), software, and data (at rest, during processing, or in transmission) through the use of access control software, rule sets, and standard configuration hardening processes.

How 1Password products/features can support SOC 2 compliance

1Password Enterprise Password Manager: Supports access management through custom groups, allowing administrators to define granular permissions that govern how users and groups interact with the tenant and its controlled content. The 1Password automated provisioning integrations enhances this by integrating with an organization's identity provider (IdP), facilitating automated and scalable user provisioning and access management.

1Password SaaS Manager: Provides features that can help organizations provision and manage user access to their applications with ability to record the how and when access was granted, including approvals from system owners and the specific level of access granted. Organizations can further configure access parameters for each application, with customizable access policies that simplify the process of granting access to tools based on teams or roles.

Additional resources

Use custom groups in 1Password Enterprise Password Manager

SOC 2 Requirement ID

CC6.1.6

Requirement description

Restricts Access to Information Assets—Combinations of data classification, separate data structures, port restrictions, access protocol restrictions, user identification, and digital certificates are used to establish access control rules for information assets.

How 1Password products/features can support SOC 2 compliance

1Password Enterprise Password Manager: Organizations can use 1Password to enforce account password requirements using via pre-made or custom policies that can applied to different groups across the organization.

Additional resources

Enforce 1Password account password requirements in 1Password Business

SOC 2 Requirement ID

CC6.1.10

Requirement description

Uses Encryption to Protect Data—The entity uses encryption to protect data (at rest, during processing, or in transmission), when such protections are deemed appropriate based on the entity's risk mitigation strategy.

How 1Password products/features can support SOC 2 compliance

1Password Enterprise Password Manager: 1Password uses end-to-end encryption and encrypts data in transit and at rest. The account password and secret key encrypt all data end-to-end, and the Secure Remote Password (SRP) reduces the risk of malicious actors stealing credentials or reading any non-secret information sent to the server.

1Password Device Trust: Data is encrypted at rest using AES 256 block-level storage encryption and TLS with modern cipher suites for data in transit.

1Password SaaS Manager: Data is encrypted at rest using AES 256-bit and TLS with modern cipher suites for data in transit.

Additional resources

About the 1Password security model

How Secure Remote Password protects your 1Password account

SOC 2 Requirement ID

CC6.1.11

Requirement description

Protects Encryption Keys—The entity protects cryptographic keys during generation, storage, use, and destruction. Cryptographic modules, algorithms, key lengths, and architectures are appropriate based on the entity's risk mitigation strategy.

How 1Password products/features can support SOC 2 compliance

1Password uses zero-knowledge encryption with AES 256-bit end to end encryption. 1Password secret keys are generated using Cryptographically Secure Pseudo-Random Number Generators (CSPRNGs). These keys are ultimately encrypted with keys derived from user secrets. All cryptographic keys are generated by the client on your devices, and all encryption is done locally.

Additional resources

About the 1Password security model

SOC 2 Requirement ID

CC6.2.1

Requirement description

Creates Access Credentials to Protected Information Assets—The entity creates credentials for accessing protected information assets based on an authorization from the system's asset owner or authorized custodian. Authorization is required for the creation of all types of credentials of individuals (for example, employees, contractors, vendors, and business partner personnel), systems, and software.

How 1Password products/features can support SOC 2 compliance

1Password SaaS Manager: Can be connected to an organization's identity provider (IdP), enabling automation of access governance processes by specifying who can request access to specific systems and how that access is approved and granted.

Additional resources

Manage access to apps

SOC 2 Requirement ID

CC6.2.2

Requirement description

Reviews Validity of Access Credentials—The entity reviews access credentials on a periodic basis for validity (for example, employees, contractors, vendors, and business partner personnel) and inappropriate system or service accounts.

How 1Password products/features can support SOC 2 compliance

1Password SaaS Manager: Offers time-based access reviews. IT Managers can schedule access reviews as one-off or recurring events, set due dates, and assign reviewer roles such as app owner or IT admin. Reviewer assignments can be manually overridden, and notifications are sent to reviewers when a review is assigned or due, and to admins when completed. Additionally SaaS Manager provides out of the box optimization workflows to continuously review access if the user hasn't logged in 30, 60 ,90 days and automatically removes access per the workflow set up.

Additional resources

Administration Access Reviews

SOC 2 Requirement ID

CC6.2.3

Requirement description

Prevents the Use of Credentials When No Longer Valid —Processes are in place to disable, destroy, or otherwise prevent the use of access credentials when no longer valid.

How 1Password products/features can support SOC 2 compliance

1Password SaaS Manager: Can be connected to an organization's identity provider (IdP) and Human Resource Information Systems (HRIS) enabling automation of access management processes by managing the process of offboarding employees and contractors from your SaaS stack and keeping records for audit purposes. An offboarding workflow can be configured to deprovision users from specific apps, including your IdP and any other apps that support deprovisioning via an integration.

Additional resources

Automate Employee Offboarding

SOC 2 Requirement ID

CC6.3.1

Requirement description

Creates or Modifies Access to Protected Information Assets—Processes are in place to create or modify access to protected information assets based on authorization from the asset's owner.

How 1Password products/features can support SOC 2 compliance

1Password SaaS Manager: Facilitates the automation of access request management by enabling organizations to predefine user permissions, approval workflows, and provisioning methods for system access. Users are able to directly request access via app catalog. For applications with suitable integrations, new user accounts are provisioned automatically for non-integrated applications, administrators can assign manual provisioning tasks to the designated app owner or IT liaison to ensure accurate monitoring and tracking of user account provisioning status through ticketing system integrations like jira.

Additional resources

Review app access risk

Manage access to apps

SOC 2 Requirement ID

CC6.3.2

Requirement description

Removes Access to Protected Information Assets—Processes are in place to remove access to protected information assets when an individual no longer requires access.

How 1Password products/features can support SOC 2 compliance

1Password SaaS Manager: The offboarding workflow is configurable to automatically deprovision users from connected applications, including the Identity Provider (IdP) and other integrated systems that support deprovisioning.

Additional resources

Automate employee offboarding

SOC 2 Requirement ID

CC6.3.3

Requirement description

Uses Access Control Structures—The entity uses access control structures, such as role-based access controls, to restrict access to protected information assets, limit privileges, and support segregation of incompatible functions.

How 1Password products/features can support SOC 2 compliance

1Password SaaS Manager: Helps automate access management by integrating with IdPs to understand user roles and permissions and enforces granular permissions that power access contol across an organization's SaaS landscape.

Additional resources

Define custom attributes and roles for apps

Manage access to apps

SOC 2 Requirement ID

CC6.3.4

Requirement description

Reviews Access Roles and Rules—The appropriateness of access roles and access rules is reviewed on a periodic basis for unnecessary and inappropriate individuals (for example, employees, contractors, vendors, business partner personnel) and inappropriate system or service accounts. Access roles and rules are modified, as appropriate.

How 1Password products/features can support SOC 2 compliance

1Password SaaS Manager: Offers time-based access reviews. IT Managers can schedule access reviews as one-off or recurring events, set due dates, and assign reviewer roles such as app owner or IT admin. Reviewer assignments can be manually overridden, and notifications are sent to reviewers when a review is assigned or due, and to admins when completed.

Additional resources

Administrating Access Reviews

SOC 2 Requirement ID

CC6.6.2

Requirement description

Protects Identification and Authentication Credentials—Identification and authentication credentials are protected during transmission outside its system boundaries.

How 1Password products/features can support SOC 2 compliance

1Password Enterprise Password Manager: 1Password uses end-to-end encryption and encrypts data in transit and at rest. The account password and secret key encrypt all data end-to-end, and the Secure Remote Password (SRP) reduces the risk of malicious actors stealing credentials or reading any non-secret information sent to the server. Additionally 1Password allows for the customers to configure their internal settings to automatically lock the application after a specified amount of time.

Additional resources

About the 1Password security model

How Secure Remote Password protects your 1Password account

SOC 2 Requirement ID

CC6.6.3

Requirement description

Requires Additional Authentication or Credentials—Additional authentication information or credentials are required when accessing the system from outside its boundaries.

How 1Password products/features can support SOC 2 compliance

1Password Enterprise Password Manager: 1Password supports many forms of multi-factor authentication (MFA) like hardware keys, Time-Based One-Time Password (TOTPs) and through integrations with MFA applications like Duo. Additionally, 1Password itself can be used to support 2FA as it can generate Time-Based One-Time Passwords (TOTPs) to be stored within the solution and auto-filled. When signing onto a new device using SSO 1Password will verify user's identity before granting access.

1Password Device Trust: Device Trust is considered a possession-based factor because it relies on the physical presence of a device that is enrolled and compliant with security policies. The device itself, which is managed and monitored by Device Trust, serves as a proof of possession, ensuring that only authorized devices can access the system.

Additional resources

Use 1Password as an authenticator for sites with two-factor authentication

SOC 2 Requirement ID

CC6.7.4

Requirement description

Protects Endpoint Devices—Processes and controls are in place to protect endpoint devices (such as mobile devices, laptops, desktops, and sensors).

How 1Password products/features can support SOC 2 compliance

1Password SaaS Manager: Connect device data from your MDM, EDR, and IT Asset Management tools to get a single, unified view of each employee and their devices.

1Password Device Trust: Helps control and monitor user-installed software by enforcing compliance through Device Trust Checks, which continuously monitor endpoint devices to detect and manage user-installed applications, ensuring only authorized software is permitted and any unauthorized installations are flagged and addressed by end users.

Additional resources

Device Trust Checks

SOC 2 Requirement ID

CC7.2.1

Requirement description

Implements Detection Policies, Procedures, and Tools—Detection policies and procedures are defined and implemented, and detection tools are implemented on Infrastructure and software to identify anomalies in the operation or unusual activity on systems. Procedures may include (1) a defined governance process for security event detection and management that includes provision of resources; (2) use of intelligence sources to identify newly discovered threats and vulnerabilities; and (3) logging of unusual system activities.

How 1Password products/features can support SOC 2 compliance

1Password Enterprise Password Manager: Business Watchtower provides organizations with visibility into password hygiene and security risks, including identifying weak, reused, or compromised passwords and highlighting applications and websites where users can enable two-factor authentication.

1Password Device Trust: Device Trust helps organizations with continuous monitoring of organizational systems and applications by providing administrators with OSQuery-based tools to perform live queries on endpoint devices. Admins can continuously monitor system configurations and software versions to detect potential vulnerabilities allowing for immediate assessment and response.

1Password SaaS Manager: 1Password SaaS Manager provides visibility into organization's SaaS ecosystem and the continuous discovery of new applications (including identification of shadow IT) and insights into user access.

Additional resources

Use Watchtower to find account details you need to change

Total Fleet Visibility in Device Trust

Get in touch with us.

Experience 1Password by requesting a demo today.