SOLUTION GUIDE

How StrongDM Helps with SOC 2 Compliance

SOC 2 is a framework developed by the American Institute of CPAs (AICPA) that specifies how software vendors and other organizations should manage customer data.

For organizations evaluating SaaS or cloud services providers, compliance with SOC 2 is a minimum requirement as it confirms to the customer that the provider has implemented certain security policies and procedures to protect customer data.

strongDM itself is SOC 2 Type 2-certified, and below are the specific requirements where strongDM can help you achieve SOC 2 certification as well.

Logical & Physical Access Controls

Requirement	Detail	strongDM Features
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.	
Identifies and Manages the Inventory of Information Assets	The entity identifies, inventories, classifies, and manages information assets.	Auto-discovery of resources such as available databases, SSH nodes, and Kubernetes clusters.
Restricts Logical Access	Logical access to information assets, including hardware, data (at-rest, during processing, or in transmission), software, administrative authorities, mobile devices, output, and offline system components is restricted through the use of access control software and rule sets.	Support for Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC) policies. Grant temporary or just-in-time access, with least-privilege by default.
Identifies and Authenticates Users	Persons, infrastructure, and software are identified and authenticated prior to accessing information assets, whether locally or remotely.	Authenticate and/or provision users & groups through your identity provider. Can also authenticate through strongDM with MFA.
Considers Network Segmentation	Network segmentation permits unrelated portions of the entity's information system to be isolated from each other.	In the strongDM architecture, resources do not connect with each other. Users can only connect to what they are given access to and are unable to elevate their privileges to move horizontally through an organization's infrastructure.

Logical & Physical Access Controls (Cont)

Requirement	Detail	strongDM Features
Manages Point Access	Points of access by outside entities and the types of data that flow through the points of access are identified, inventoried, and managed. The types of individuals and systems using each point of access are identified, documented, and managed.	Manage and audit all activities, whether employees, contractors, or other third-parties, regarding access to backend infrastructure.
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.	strongDM uses a combination of user identities, network segmentation (making only gateways public), and roles/groups to generate and enforce access control rules.
Manages Identification and Authentication	Identification and authentication requirements are established, documented, and managed for individuals and systems accessing entity information, infrastructure, and software.	Federate with your identity provider or use strongDM's native authentication, which allows administrators to set minimum password requirements.
Manages Credentials for Infrastructure and Software	New internal and external infrastructure and software are registered, authorized, and documented prior to being granted access credentials and implemented on the network or access point. Credentials are removed and access is disabled when access is no longer required or the infrastructure and software are no longer in use.	Store credentials in a hardened AWS vault or configure your own secret store to work with strongDM.
Uses Encryption to Protect Data	The entity uses encryption to supplement other measures used to protect data at rest, when such protections are deemed appropriate based on assessed risk.	All connections are encrypted using TLS 1.2.
Protects Encryption Keys	Processes are in place to protect encryption keys during generation, storage, use, and destruction.	All secrets and credentials are obfuscated with encryption keys stored in a hardened vault.
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.	
Controls Access Credentials to Protected Assets	Information asset access credentials are created based on an authorization from the system's asset owner or authorized custodian.	Credentials are never provided to the end user. The gateway authenticates to the final resource in the last hop using stored credentials, which are stored securely with strongDM or with an existing secrets manager (HashiCorp Vault, AWS Secrets Manager, GCP Secret Manager).
Removes Access to Protected Assets When Appropriate	Processes are in place to remove credential access when an individual no longer requires such access.	Instantly grant and revoke permanent or just-in-time access to resources through the strongDM admin UI or through your identity provider.
Reviews Appropriateness of Access Credentials	The appropriateness of access credentials is reviewed on a periodic basis for unnecessary and inappropriate individuals with credentials.	The strongDM admin UI maintains a list of all users and resources they have access to. Admins can define and enforce the appropriate access policies based on a user's role or a resource's attributes with comprehensive permissions auditing available.

Logical & Physical Access Controls (Cont)

Requirement	Detail	strongDM Features
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.	
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.	User access privileges are derived from their assigned roles with the exception of "temporary access" and "no role assigned." The strongDM AccessBot can also be used to grant temporary access within applications like Slack and Microsoft Teams.
Removes Access to Protected Information Assets	Processes are in place to remove access to protected information assets when an individual no longer requires access.	strongDM enables admins to revoke access instantly or on a time-bound basis (i.e., temporary access).
Uses Role-Based Access Controls	Role-based access control is utilized to support segregation of incompatible functions.	strongDM admins grant access based on roles (i.e., role-based access control).
Reviews Access Roles and Rules	The appropriateness of access roles and access rules is reviewed on a periodic basis for unnecessary and inappropriate individuals with access and access rules are modified as appropriate.	Administrators can use the strongDM CLI to view users, roles, and access at any time over the past 13 months, providing both current and historical "point in time" access details.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	
Restricts Access	The types of activities that can occur through a communication channel (for example, FTP site, router port) are restricted.	Configuring a data source with a particular driver restricts the communication over that connection to that specific driver protocol. SSH cannot be tunneled through a port set up for MySQL, for instance.
Protects Identification and Authentication Credentials	Identification and authentication credentials are protected during transmission outside its system boundaries.	All connectivity between strongDM components (Client, Gateway, API) are encrypted in transit.
Requires Additional Authentication or Credentials	Additional authentication information or credentials are required when accessing the system from outside its boundaries.	As an additional layer of security, strongDM supports MFA through an organization's identity provider or via Duo in strongDM.
Implements Boundary Protection Systems	Boundary protection systems (e.g., firewalls, demilitarized zones, and intrusion detection systems) are implemented to protect external access points from attempts and unauthorized access and are monitored to detect such attempts.	By deploying strongDM gateways and relays, customers can make all of their resources "internal-only" and not visible through their system boundary.
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.	
Uses Encryption Technologies or Secure Communication Channels to Protect Data	Encryption technologies or secured communication channels are used to protect transmission of data and other communications beyond connectivity access points.	All connectivity between strongDM components (Client, Gateway, API) are encrypted in transit.

System Operations

Requirement	Detail	strongDM Features
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.	
Monitors Infrastructure and Software	The entity monitors infrastructure and software for noncompliance with the standards, which could threaten the achievement of the entity's objectives.	By logging all of the commands that are run on target systems and exporting strongDM logs to a SIEM, customers can detect potential areas of noncompliance.
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.	
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.	strongDM captures every action, including every user, authentication, query, SSH, and RDP command as well as administrator actions such as permissions changes.
Designs Detection Measures	Detection measures are designed to identify anomalies that could result from actual or attempted (1) compromise of physical barriers; (2) unauthorized actions of authorized personnel; (3) use of compromised identification and authentication credentials; (4) unauthorized access from outside the system boundaries; (5) compromise of authorized external parties; and (6) implementation or connection of unauthorized hardware and software.	strongDM's audit logs can be automatically streamed to a SIEM of your choice to facilitate anomaly detection.
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.	
Communicates and Reviews Detected Security Events	Detected security events are communicated to and reviewed by the individuals responsible for the management of the security program and actions are taken, if necessary.	Centralized audit logs enable easy, fast investigations of security incidents.
Develops and Implements Procedures to Analyze Security Incidents	Procedures are in place to analyze security incidents and determine system impact.	strongDM provides robust audit logs for all access to configured data sources, which can assist in evaluations and investigations of security incidents.
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.	
Contains Security Incidents	Procedures are in place to contain security incidents that actively threaten entity objectives.	strongDM enables admins to immediately revoke access to systems/data sources for accounts that may be compromised.
Mitigates Ongoing Security Incidents	Procedures are in place to contain security incidents that actively threaten entity objectives.	strongDM enables admins to immediately revoke access to systems/data sources for accounts that may be compromised.

System Operations (Cont)

Requirement	Detail	strongDM Features
Ends Threats Posed by Security Incidents	Procedures are in place to end the threats posed by security incidents through closure of the vulnerability, removal of unauthorized access, and other remediation actions.	strongDM enables admins to immediately revoke access to systems/data sources for accounts that may be compromised.
Obtains Understanding of Nature of Incident and Determines Containment Strategy	An understanding of the nature (for example, the method by which the incident occurred and the affected system resources) and severity of the security incident is obtained to determine the appropriate containment strategy, including (1) a determination of the appropriate response time frame, and (2) the determination and execution of the containment approach.	strongDM provides comprehensive audit logs for all access to configured data sources, which are critical in security incident investigations.
Evaluates the Effectiveness of Incident Response	The design of incident-response activities is evaluated for effectiveness on a periodic basis.	Periodically review audit logs and session recordings to identify potential gaps in your incident response plan and adjust accordingly to enhance effectiveness.
Periodically Evaluates Incidents	Periodically, management reviews incidents related to security, availability, processing integrity, confidentiality, and privacy and identifies the need for system changes based on incident patterns and root causes.	Review audit logs and session recordings to identify opportunities to improve security posture.
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	
Determines Root Cause of the Event	The root cause of the event is determined.	strongDM provides session recordings and audit logs for all access to configured data sources, which are critical for identifying root cause in security incidents.
Improves Response and Recovery Procedures	Lessons learned are analyzed and the incident-response plan and recovery procedures are improved.	Use audit logs to analyze incidents and to develop appropriate responses.

Change Management

Requirement	Detail	strongDM Features
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.	
Provides for Changes Necessary in Emergency Situations	A process is in place for authorizing, designing, testing, approving, and implementing changes necessary in emergency situations (that is, changes that need to be implemented in an urgent time frame).	Grant temporary or just-in-time access, with least-privilege by default. Integrate your PagerDuty on-call schedule with strongDM to automatically grant strongDM users access to additional resources during their on-call shifts. The strongDM AccessBot can also be used to grant temporary access within applications like Slack and Microsoft Teams.