SOLUTION GUIDE

How StrongDM Helps with FedRAMP

strongdm

The Federal Risk and Authorization Management Program (FedRAMP) is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services. StrongDM provides the foundation to meet FedRAMP requirements for Access Control, Audit and Accountability, Identification and Authentication, Incident Response, Personnel Security, Risk Assessment, and System and Communications Protection.

Below are the specific requirements where StrongDM can help you meet to become FedRAMP authorized.

Control Family: Access Control

Control Name & ID	Assessment Objective	StrongDM Capability
Account Management AC-2 | AC-02i.01 IMPACT LEVEL: High Moderate Low	Determine if access to the system is authorized based on a valid access authorization	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.
Account Management AC-2 | AC-02i.03 IMPACT LEVEL: High Moderate Low	Determine if access to the system is authorized based on organization-defined attributes	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.
Account Management AC-2(7) | AC-02(07)(d) IMPACT LEVEL: High Moderate	Determine if access is revoked when privileged role or attribute assignments are no longer appropriate	Instantly revoke permanent or Just-in-time access to resources through the StrongDM admin UI or through your identity provider. Access to critical infrastructure aligns with the identity lifecycle, permissions occur only through StrongDM which authenticates the users through your identity provider or through StrongDM with MFA.
Account Management AC-3 | AC-03 IMPACT LEVEL: High Moderate Low	Determine if approved authorizations for logical access to information and system resources are enforced in accordance with applicable access control policies	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.

Control Family: Access Control		
Control Name & ID	**Assessment Objective**	**StrongDM Capability**
Least Privilege AC-6 | AC-06 IMPACT LEVEL: High Moderate	Determine if the principle of least privilege is employed, allowing only authorized accesses for users (or processes acting on behalf of users) that are necessary to accomplish assigned organizational tasks	Grant temporary or Just-in-Time access, with least privilege by default, for managing access to critical infrastructure. Integrate testing, approving, and implementing changes necessary in emergency situations (e.g. grant temporary access within applications like Slack and Microsoft Teams). Eliminate Standing Privileges and grant access through workflows. The Access Workflows report shows the number of access requests and workflows being used at any given time. In addition, the Standing Access Report provides information about access grants that have been inactive for a certain period of time, displaying information such as the user's name, the name and type of resource they were granted access, and the last time the resource was accessed. This report allows admins to easily see which users are not using the resources available to them, and assess whether or not their access should be revoked.
Log Use of Privileged Functions AC-6 (9) | AC-06(09) IMPACT LEVEL: High Moderate	Determine if the execution of privileged functions is logged	StrongDM provides session recordings and audit logs for all access to configured data sources, which are critical for identifying root cause in security incidents. Additionally, the Executive Summary report shows an overview of all user activity, grant utilization, and resource utilization. Understand exactly which roles are accessing which resources.
Session Termination AC-12 | AC-12 IMPACT LEVEL: High Moderate	Determine if a user session is automatically terminated after [organization-defined conditions or trigger events]	Sessions can be terminated by StrongDM admins or approvers directly from the Admin UI at any given time. Access is automatically revoked when a users role changes in the integrated Identity Provider or if there is a suspicious context-signal. For example, Device Trust provides a context signals when verfying a user. Trust the user, trust the device, and then grant access and authorization to continue operations. This feature provides a deeper context for every access request by analyzing the risk profile of the device utilized for the request. Organizations can ensure that only those devices that meet their device security and health requirements are allowed to connect for privileged operations.
Remote Access AC-17 | AC-17b IMPACT LEVEL: High Moderate Low	Determine if each type of remote access to the system is authorized prior to allowing such connections	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.

Control Family: Access Control

Control Name & ID	Assessment Objective	StrongDM Capability
Monitoring and Control AC-17 (1) | AC-17(01) IMPACT LEVEL: High Moderate	Determine if automated mechanisms are employed to monitor and control remote access methods	Log all commands that are run on target systems and export StrongDM logs to an S3 Bucket or a SIEM/SOAR solution.
Managed Access Control Points AC-17 (3) | AC-17(04)(a)[01][03] IMPACT LEVEL: High Moderate	Determine if remote accesses are routed through authorized and managed network access control points	StrongDM uses network segmentation, and only makes gateways public, to generate and enforce access control rules.
Privileged Commands and Access AC-17 (4) | AC-17(04)(a)[01][03] IMPACT LEVEL: High Moderate	Determine if the execution of privileged commands via remote access is authorized only in a format that provides assessable evidence and is authorized only for the following needs: [organization-defined needs requiring remote access]	StrongDM provides session recordings and audit logs for all access to configured data sources, which are critical for identifying root cause in security incidents.
Privileged Commands and Access AC-17 (4) | AC-17(04)(a)[01][04] IMPACT LEVEL: High Moderate	Determine if access to security-relevant information via remote access is authorized only in a format that provides assessable evidence and is authorized only for the following needs: [organization-defined needs requiring remote access]	StrongDM provides session recordings and audit logs for all access to configured data sources, which are critical for identifying root cause in security incidents.

Control Family: Audit and Accountability

Control Name & ID	Assessment Objective	StrongDM Capability
Event Logging AU-2 | AU-02c.[02] IMPACT LEVEL: High Moderate Low	Determine if the specified event types are logged within the system [organization-defined frequency or situation]	StrongDM provides session recordings and audit logs for all access to configured data sources, which are critical for identifying root cause in security incidents. Log all commands that are run on target systems and export StrongDM logs to an S3 Bucket or a SIEM/SOAR solution.
Content of Audit Records AU-3 | AU-03 IMPACT LEVEL: High Moderate Low	Determine if audit records contain information that establishes: • what type of event occurred; • when the event occurred; • where the event occurred; • the source of the event; • the outcome of the event; • the identity of any individuals, subjects, or objects/entities associated with the event	StrongDM provides session recordings and audit logs for all access to configured data sources, which are critical for identifying root cause in security incidents. Log all commands that are run on target systems and export StrongDM logs to an S3 Bucket or a SIEM/SOAR solution.

Control Family: Audit and Accountability		
Control Name & ID	**Assessment Objective**	**StrongDM Capability**
Audit Record Retention AU-11 | AU-11 IMPACT LEVEL: High Moderate Low	Determine if audit records are retained for [organization-defined time period consistent with records retention policy] to provide support for after-the-fact investigations of incidents and to meet regulatory and organizational information retention requirements	All logs can be stored for 13 months or streamed to an S3 bucket or SIEM/SOAR solution.

Control Family: Identification and Authentication		
Identification and Authentication (Organizational Users) IA-2 | IA-02[01] IMPACT LEVEL: High Moderate Low	Determine if organizational users are uniquely identified and authenticated	Access to critical infrastructure aligns with the identity lifecyle, permissions occur only through StrongDM which authenticates the users through your identity provider or through StrongDM with MFA.
Multi-factor Authentication to Privileged Accounts IA-2 (1) | IA-02(01) IMPACT LEVEL: High Moderate Low	Determine if multi-factor authentication is implemented for access to privileged accounts	Access to critical infrastructure aligns with the identity lifecyle, permissions occur only through StrongDM which authenticates the users through your identity provider or through StrongDM with MFA.

Control Family: Incident Response		
Exposure to Unauthorized Personnel IR-9 (4) | IR-9 (04) IMPACT LEVEL: High Moderate	Determine if [organization-defined controls] are employed for personnel exposed to information not within assigned access authorizations	Access to critical infrastructure aligns with the identity lifecyle, permissions occur only through StrongDM which authenticates the users through your identity provider or through StrongDM with MFA. Additionally, grant temporary or Just-in-Time access, with least privilege by default, for managing access to critical infrastructure. Implement Zero Standing Privileges with Access Workflows and Dynamic Access Rules, so that authorization grants are approved and granted only when needed.

Control Family: Personnel Security		
Personnel Termination PS-4 | PS-04a IMPACT LEVEL: High Moderate Low	Determine if upon termination of individual employment, system access is disabled within [organization-defined time period]	Access to critical infrastructure aligns with the identity lifecyle, permissions occur only through StrongDM which authenticates the users through your identity provider or through StrongDM with MFA.

Control Family: Personnel Security		
Control Name & ID	**Assessment Objective**	**StrongDM Capability**
Automated Actions PS-4 (2) | PS-04 (02) IMPACT LEVEL: High	Determine if [organization-defined automated mechanisms] are used to [organization-defined selection: notify organization-defined personnel or roles of individual termination actions; disable access to system resources]	Access to critical infrastructure aligns with the identity lifecyle, permissions occur only through StrongDM which authenticates the users through your identity provider or through StrongDM with MFA. StrongDM's Access Workflows solution provides a comprehensive, auditable, and streamlined approach to managing user access rights and permissions through requests that grant access through automated or human approval.
Personnel Transfer PS-5 | PS-05a IMPACT LEVEL: High Moderate Low	Determine if the ongoing operational need for current logical and physical access authorizations to systems and facilities are reviewed and confirmed when individuals are reassigned or transferred to other positions within the organization	Access to critical infrastructure aligns with the identity lifecyle, permissions occur only through StrongDM which authenticates the users through your identity provider or through StrongDM with MFA.
Control Family: Risk Assessment		
Privileged Access RA-5 (5) | RA-05 (05) IMPACT LEVEL: High Moderate	Determine if privileged access authorization is implemented to [organization-defined system components] for [organization-defined vulnerability scanning activities]	StrongDM's Access Workflows solution provides a comprehensive, auditable, and streamlined approach to managing user access rights and permissions through requests that grant access through automated or human approval.
Control Family: System and Communications Protection		
Route Traffic to Authenticated Proxy Servers SC-7 (8) | SC-07 (08) IMPACT LEVEL: High Moderate	Determine if [organization-defined internal communications traffic] is routed to [organization-defined external networks] through authenticated proxy servers at managed interfaces	StrongDM uses network segmentation, and only makes gateways public, to generate and enforce access control rules.
Network Disconnect SC-10 | SC-10 IMPACT LEVEL: High Moderate	Determine if the network connection associated with a communication session is terminated at the end of the session or after [organization-defined time period] of inactivity	Grant temporary or Just-in-Time access, with least privilege by default, for managing access to critical infrastructure. Integrate testing, approving, and implementing changes necessary in emergency situations (e.g. grant temporary access within applications like Slack and Microsoft Teams). Sessions are terminated at the time time bound access grants expire.
Control Family: System and Information Integrity		
Privileged Users SI-4 (20) | SI-04 (20) IMPACT LEVEL: High	Determine if [organization-defined additional monitoring] of privileged users is implemented	StrongDM provides session recordings and audit logs for all access to configured data sources, which are critical for identifying root cause in security incidents. Analytics Dashboards give granualr information on all role utilization, user activity, grant utlization, and available temporary access grants.