SOLUTION GUIDE

How StrongDM Helps with AWS Well-Architected Framework

The AWS Well-Architected Framework designed by AWS helps cloud architects build secure, high-performing, resilient, and efficient infrastructure for a variety of applications and workloads.

Below are the specific requirements where StrongDM can help you achieve the Security and Reliability pillar.

Best Practice	Description	How StrongDM Helps
Security: Identity and Access Management		
SEC 02	**How do you manage identities for people and machines?** There are two types of identities you need to manage when approaching operating secure AWS workloads. Understanding the type of identity you need to manage and grant access helps you ensure the right identities have access to the right resources under the right conditions. Human Identities: Your administrators, developers, operators, and end users require an identity to access your AWS environments and applications. These are members of your organization, or external users with whom you collaborate, and who interact with your AWS resources via a web browser, client application, or interactive command-line tools. Machine Identities: Your service applications, operational tools, and workloads require an identity to make requests to AWS services—for example, to read data. These identities include machines running in your AWS environment such as Amazon EC2 instances or AWS Lambda functions. You may also manage machine identities for external parties who need access. Additionally, you may also have machines outside of AWS that need access to your AWS environment.	
SEC02-BP01 Use strong sign-in mechanisms	Sign-ins (authentication using sign-in credentials) can present risks when not using mechanisms like multi-factor authentication (MFA), especially in situations where sign-in credentials have been inadvertently disclosed or are easily guessed. Use strong sign-in mechanisms to reduce these risks by requiring MFA and strong password policies.	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.

Best Practice	Description	How StrongDM Helps
SEC02-BP02 Use temporary credentials	When doing any type of authentication, it's best to use temporary credentials instead of long-term credentials to reduce or eliminate risks, such as credentials being inadvertently disclosed, shared, or stolen.	StrongDM eliminates credential exposure from all end users when connecting to resources. End users simply log into the client and connect. Authentication occurs with an identify provider or through StrongDM with MFA.
SEC02-BP03 Store and use secrets securely	A workload requires an automated capability to prove its identity to databases, resources, and third-party services. This is accomplished using secret access credentials, such as API access keys, passwords, and OAuth tokens. Using a purpose-built service to store, manage, and rotate these credentials helps reduce the likelihood that those credentials become compromised.	StrongDM stores credentials in a hardened AWS vault. We also support customer-owned-and-maintained secret stores that can be configured for access.
SEC02-BP04 Rely on a centralized identity provider	For workforce identities, rely on an identity provider that enables you to manage identities in a centralized place. This makes it easier to manage access across multiple applications and services, because you are creating, managing, and revoking access from a single location. For example, if someone leaves your organization, you can revoke access for all applications and services (including AWS) from one location. This reduces the need for multiple credentials and provides an opportunity to integrate with existing human resources (HR) processes.	StrongDM's SCIM integration with Identity Providers enables all user and group permissions to be synced directly with StrongDM.
SEC02-BP05 Audit and rotate credentials periodically	Audit and rotate credentials periodically to limit how long the credentials can be used to access your resources. Long-term credentials create many risks, and these risks can be reduced by rotating long-term credentials regularly.	StrongDM never exposes credentials to end users. Leverage StrongDM's Access Workflows to implement just-in-time access to all infrastructure to eliminate standing access and reach Zero Standing Privileges.
SEC02-BP06 Leverage user groups and attributes	As the number of users you manage grows, you will need to determine ways to organize them so that you can manage them at scale. Place users with common security requirements in groups defined by your identity provider, and put mechanisms in place to ensure that user attributes that may be used for access control (for example, department or location) are correct and updated. Use these groups and attributes to control access, rather than individual users. This allows you to manage access centrally by changing a user's group membership or attributes once with a permission set, rather than updating many individual policies when a user's access needs change.	Access to critical infrastructure aligns with the identity lifecyle, all user roles and groups are synced from the identity provder directly into StrongDM.

Best Practice	Description	How StrongDM Helps
Security: Identity and Access Management		
SEC 03	**How do you manage permissions for people and machines?** Manage permissions to control access to people and machine identities that require access to AWS and your workload. Permissions control who can access what, and under what conditions.	
SEC03-BP01 Define access requirements	Each component or resource of your workload needs to be accessed by administrators, end users, or other components. Have a clear definition of who or what should have access to each component, choose the appropriate identity type and method of authentication and authorization.	Access can be granted through role-based access, attribute-based access or time-bound. All access activity is available in StrongDM's Access Review report ensuring proper access hygiene is met.
SEC03-BP02 Grant least privilege access	It's a best practice to grant only the access that identities require to perform specific actions on specific resources under specific conditions. Use group and identity attributes to dynamically set permissions at scale, rather than defining permissions for individual users. For example, you can allow a group of developers access to manage only resources for their project. This way, if a developer leaves the project, the developer's access is automatically revoked without changing the underlying access 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.
SEC03-BP03 Establish emergency access process	A process that allows emergency access to your workload in the unlikely event of an automated process or pipeline issue. This will help you rely on least privilege access, but ensure users can obtain the right level of access when they require it. For example, establish a process for administrators to verify and approve their request, such as an emergency AWS cross-account role for access, or a specific process for administrators to follow to validate and approve an emergency request.	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.
SEC03-BP04 Reduce permissions continuously	As your teams determine what access is required, remove unneeded permissions and establish review processes to achieve least privilege permissions. Continually monitor and remove unused identities and permissions for both human and machine access.	The StrongDM Least Privilege Report identifies all unused privilged a certain duration. Revoke unused access or make modifications to roles or tags based on access activity.
SEC03-BP05 Define permission guardrails for your organization	Establish common controls that restrict access to all identities in your organization. For example, you can restrict access to specific AWS Regions, or prevent your operators from deleting common resources, such as an IAM role used for your central security team.	Resource attributes can be defined using StrongDM's tagging capabilities, and those tags can be used to define access grants by location, resource type, or more.

Best Practice	Description	How StrongDM Helps
SEC03-BP08 Share resources securely within your organization	As the number of workloads grows, you might need to share access to resources in those workloads or provision the resources multiple times across multiple accounts. You might have constructs to compartmentalize your environment, such as having development, testing, and production environments. However, having separation constructs does not limit you from being able to share securely. By sharing components that overlap, you can reduce operational overhead and allow for a consistent experience without guessing what you might have missed while creating the same resource multiple times.	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.
SEC03-BP09 Share resources securely with a third party	The security of your cloud environment doesn't stop at your organization. Your organization might rely on a third party to manage a portion of your data. The permission management for the third-party managed system should follow the practice of just-in-time access using the principle of least privilege with temporary credentials. By working closely with a third party, you can reduce the scope of impact and risk of unintended access together.	Manage third-party access to critical infrastructure with temporary access grants that are defined my role, attributes, or project duration. Access can be managed through StrongDM or ChatOps tools like Slack or Microsoft Teams.
SEC03-BP06 Manage access based on life cycle	Integrate access controls with operator and application lifecycle and your centralized federation provider. For example, remove a user's access when they leave the organization or change roles.	Access to critical infrastructure aligns with the identity lifecyle, permissions occur only through StrongDM which authenticates the users through your identity provider. Any user changes in groups and roles are immediately reflected in StrongDM.
Security: Detection		
SEC 04	**How do you detect and investigate security events?** Capture and analyze events from logs and metrics to gain visibility. Take action on security events and potential threats to help secure your workload.	
SEC04-BP01 Configure service and application logging	Retain security event logs from services and applications. This is a fundamental principle of security for audit, investigations, and operational use cases, and a common security requirement driven by governance, risk, and compliance (GRC) standards, policies, and procedures.	Log all commands that are run on target systems and export StrongDM logs to an S3 Bucket or a SIEM/SOAR solution.

Best Practice	Description	How StrongDM Helps
Security: Infrastructure Protection		
SEC 06	**How do you protect your compute resources?**	
SEC06-BP05 Enable people to perform actions at a distance	Removing the ability for interactive access reduces the risk of human error, and the potential for manual configuration or management. For example, use a change management workflow to deploy Amazon Elastic Compute Cloud (Amazon EC2) instances using infrastructure-as-code, then manage Amazon EC2 instances using tools such as AWS Systems Manager instead of allowing direct access or through a bastion host. AWS Systems Manager can automate a variety of maintenance and deployment tasks, using features including automation workflows, documents (playbooks), and the run command. AWS CloudFormation stacks build from pipelines and can automate your infrastructure deployment and management tasks without using the AWS Management Console or APIs directly.	StrongDM is a Dynamic Access Management platform that grants access to users only when they need it through just in time access grants. Cloud resources can be configured to use StrongDM's dynamic access capabilities with the AWS CLI and AWS SDKs.
Security: Data Protection		
SEC 08	**How do you protect your data at rest?**	
SEC08-BP05 Use mechanisms to keep people away from data	Keep all users away from directly accessing sensitive data and systems under normal operational circumstances. For example, use a change management workflow to manage Amazon Elastic Compute Cloud (Amazon EC2) instances using tools instead of allowing direct access or a bastion host. This can be achieved using AWS Systems Manager Automation, which uses automation documents that contain steps you use to perform tasks. These documents can be stored in source control, be peer reviewed before running, and tested thoroughly to minimize risk compared to shell access. Business users could have a dashboard instead of direct access to a data store to run queries. Where CI/CD pipelines are not used, determine which controls and processes are required to adequately provide a normally disabled break-glass access mechanism.	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.

Best Practice	Description	How StrongDM Helps
Security: Incident Response		
SEC 10	**How do you anticipate, respond to, and recover from incidents?**	
SEC10-BP05 Pre-provision access	Verify that incident responders have the correct access pre-provisioned in AWS to reduce the time needed for investigation through to recovery.	With StrongDM Access Workflows grant access to resources based on role that are automated or require human approval. Incident responders are granted time bound access to resources for the duration of the investigation. All access is revoked with then investigation is complete.
Reliability: Failure Management		
REL 09	**How do you back up data?**	
REL09-BP02 Secure and encrypt backups	Control and detect access to backups using authentication and authorization. Prevent and detect if data integrity of backups is compromised using encryption.	The StrongDM implementation fully leverages authenticated encryption with associated data (AEAD) via the KMS Encryption Context. All credential decryption events are written to a tamper-hardened audit log that is owned by a separate AWS account. Your gateway is the only thing that can decrypt credentials on an end user's behalf.