SOLUTION GUIDE

How StrongDM Helps with Cyber Insurance

Cyber insurance provides coverage for the losses an organization might suffer from a data breach or cyber attack.

Below are common requirements for qualifying for cyber insurance and how StrongDM can help your organization meet those requirements.

Requirement	Description	StrongDM for Cyber Insurance
Privileged Access Management (PAM)	Applicant must demonstrate use of privileged access management, including verifying the use of a tool or software solution for PAM. Applicant must also confirm that they use unique, privileged credentials for admin tasks (separate from every day credentials, such as emails).	When using StrongDM, privileged credentials are managed completely separate from the end user and end-user workstation, eliminating the ability of the end user to replicate passwords and credentials for admin tasks. Credentials stored in StrongDM are never exposed to the users.
Privilege Escalation	Applicant must show controls in place to prevent privilege escalation.	You can easily implement least privilege by providing right-size access based on the user, role, and access controls (RBAC, ABAC, PBAC) with StrongDM. As a result, even if an end-user's credentials were used to gain improper access, it would not be possible to escalate privileges without going through an approved access workflow which would extend the privileges.
Account & Asset Inventories	Applicant must verify that they maintain an inventory of IT assets (hardware and software), and user and admin accounts, including name, username, start/stop dates, and department.	StrongDM maintains a comprehensive list of resources, users and their associated access. This user list can be integrated with the organization's identity provider to ensure that access is provisioned and deprovisioned as employees join, leave, or change roles. StrongDM also maintains an inventory of all resources that have access managed through the platform.

Requirement	Description	StrongDM for Cyber Insurance
Least Privilege	Applicant must verify that access to the network, as well as personal, corporate, and sensitive information, is restricted on a least privilege basis.	StrongDM inherently implements the principle of least privilege by providing right-size access based on the user, his/her role, and access controls (RBAC, ABAC, PBAC). These access controls may be applied to any user in the organization ensuring that least privilege is implemented across all sensitive resources.
Multi-Factor Authentication	Applicant must confirm the usage of multi-factor authentication for domain accounts, remote access (for employees and third parties), and for their PAM.	StrongDM uses robust, standards-based, phishing-resistant multi-factor authentication mechanisms. StrongDM extends beyond the conventional approach of validating identity during initial access by continuously verifying user identity, thereby ensuring ongoing validation in line with Zero Trust.
Access Audits	Applicant must verify that access is audited and updated, including validating that active accounts are authorized on a quarterly basis. This audit must include the exercise of admin and privileged access, and confirm that all accounts associated with critical processes are current users.	StrongDM's Advanced Insights feature provides analytics and reporting for credentials and sensitive resource usage. This includes when every credential was last used, and when each system was last accessed. Activity and audit data can be maintained in the platform or streamed/exported to other security analytics or logging platforms. StrongDM's native reporting capabilities help surface access grants and activities that may require further investigation and remediation.
Processes & Approvals	Applicant must show processes in place for access requests and provide where senior management approval is required for access.	StrongDM provides a variety of options for access request and approval workflows. Requests can follow predefined business rules to automatically provide access, or be routed to the appropriate manager or stakeholder for review.
Just-in-Time Access	Applicant must verify that accounts are managed and monitored through Just-in-Time access, credentials are time bound, and require necessary approvals for privileged access.	Access provided by StrongDM is inherently provided in a just-in-time and time-bound fashion. Because StrongDM is a protocol-aware proxy, credentials are injected during the "last mile" hop between the proxy and the target database, server or other resource. As a result, sensitive credentials are always inaccessible to users: they are never transferred to a client in any form. Furthermore, access may be revoked at any time by an admin.

Requirement	Description	StrongDM for Cyber Insurance
Domain/Service Accounts	Applicant must confirm that human and non-human accounts abide by least privilege at all times. Applicant must also detail how domain administrator access is controlled and what safeguards are in place regarding IT network administration.	StrongDM simply treats domain and service accounts as users within the platform. That means these credentials receive the same safeguards, access controls, and processes as users within the platform.
Remote Access	Applicant must provide the protections that exist in order to prevent remote access to corporate networks.	StrongDM can be used alongside, or in lieu of, a VPN to manage remote access to corporate networks. StrongDM establishes fully distributed ingress/egress micro-perimeters and extensive micro-segmentation based on user access profiles. This approach allows for dynamic just-in-time, and just-enough connectivity for each session, enhancing service-specific interconnections while ensuring isolated and secure communication pathways.
Break Glass	Applicant must confirm that a backup plan exists in the case that an attack renders privileged accounts and passwords inaccessible.	StrongDM provides break-glass guidance for organizations to be able to maintain access to critical accounts in the case of an emergency of when an attack renders systems inaccessible.
Credential Monitoring	Applicant must verify which type of credential monitoring has been implemented to track privileged account usage.	StrongDM creates an audit trail of all access and activities, helping organizations track and monitor the actions of employees/contractors as they begin using critical resources. The platform's observability includes meticulous user activity logging and subsequent analysis. Behavior-centric analytics contributes to situational awareness across the enterprise, a pivotal component of Zero Trust's analytical approach to security.