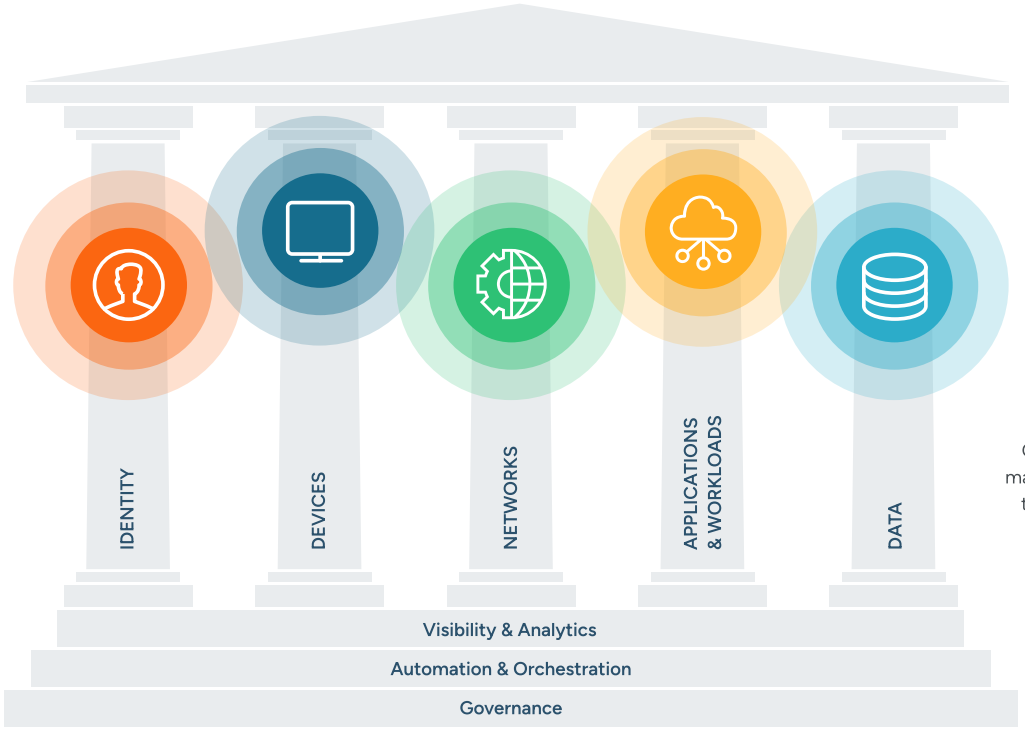
SOLUTION GUIDE

How StrongDM Helps with the CISA Zero Trust Maturity Model

The Cybersecurity and Infrastructure Security Agency (CISA) Zero Trust Maturity Model (ZTMM) lays out a framework for practically achieving Zero Trust. While originally intended for government agencies, the ZTMM has wide applicability, including as a potential roadmap for large enterprises to achieve Zero Trust.

The ZTMM breaks the requirements of Zero Trust into five categories across three foundational needs (see image below; *source: Zero Trust Maturity Model, April 2023; CISA Cybersecurity Division*).



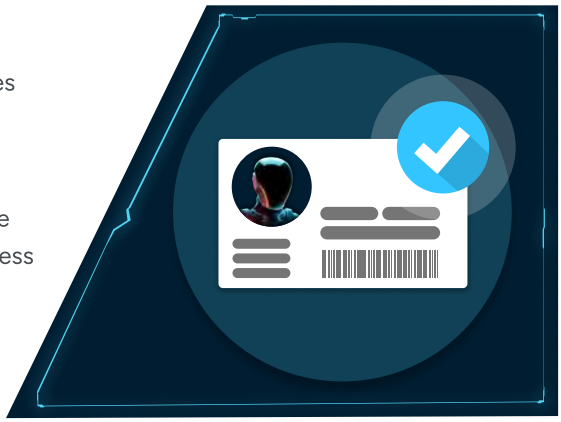
CISA's ZTMM is one of many paths to support the transition to zero trust.

StrongDM & the CISA ZTMM

StrongDM delivers a dynamic access management platform that can support your organization's ZTMM efforts. The platform addresses key requirements of the Identity and Networks pillars, and plays a critical role in enabling your organization to deliver secure access across all of your technical users. Access provided via StrongDM is secure, auditable, and delivered in a Just-in-Time manner, ensuring that access is only available when, where, and to whom it is needed, and doesn't exist when it does not.

Below is a breakdown of how StrongDM specifically supports both pillars.

5.1 Identity



The first pillar of the ZTMM is identity. This refers to “an attribute or set of attributes that uniquely describes an agency user or entity, including non-person entities.”

The identity pillar is focused on enforcing user and entity access to the right resources, at the right time, for the right purpose—all without over provisioning the user. This is accomplished through the combination of identity, credential, and access management solutions that enforce strong authentication, context-based authorization, and that assess the risk of users.

StrongDM & Identity

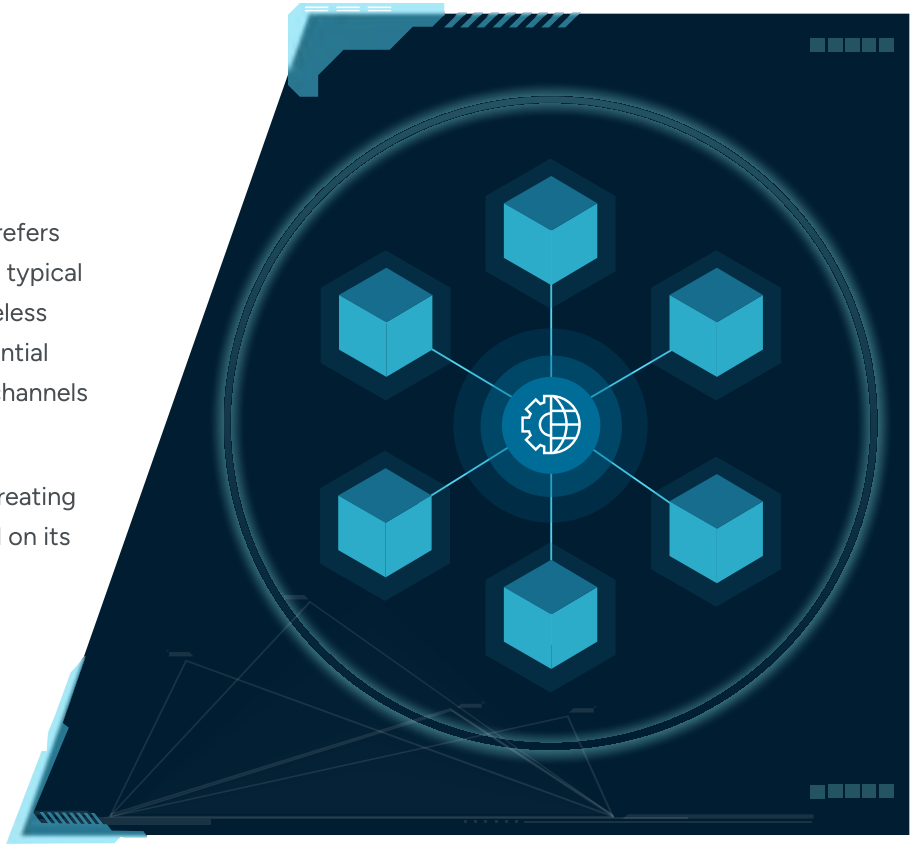
Function	Optimal Requirements	How Strong DM Supprts
Authentication	Agency continuously validates identity with phishing-resistant MFA, not just when access is initially granted.	The StrongDM platform utilizes robust, standards-based, phishing-resistant multi-factor authentication mechanisms. StrongDM extends beyond the conventional approach of validating identity during initial access by continuously verifying user identity, thereby ensuring ongoing validation in line with the Zero Trust principle.
Identity Stores	Agency securely integrates their identity stores across all partners and environments as appropriate.	A key differentiated strength of StrongDM lies in its ability to seamlessly integrate with diverse identity stores and secret vaults across varied environments. StrongDM is a protocol-aware proxy and injects credentials during the “last mile” hop between the proxy and the target web application, database, server, cluster, or cloud resource. As a result, sensitive credentials are always inaccessible to users and never transferred to a StrongDM client in any form. Once needed, credentials are unlocked at runtime using a “dual-key” system. The following must be true for credentials to be unlocked: a cryptographically valid proxy instance requests decryption on behalf of a cryptographically valid user session. Neither the user nor the proxy instance alone can decrypt a credential. This practice centralizes identity management and also heightens organizational awareness of enterprise identities and their corresponding roles.
Risk Assessments	Agency determines identity risk in real time based on continuous analysis and dynamic rules to deliver ongoing protection.	StrongDM employs a sophisticated framework of continuous, dynamic analysis and rules to evaluate access risk in real-time. This real-time risk assessment aligns with Zero Trust, which involves making access determinations based on contextual insights and user behavior.
Access Management (New Function)	Agency uses automation to authorize just-in-time and just-enough access tailored to individual actions and individual resource needs.	At the core of StrongDM's functionality is the capability to facilitate precisely timed and precisely scoped access. The platform orchestrates access through automated processes and workflows, ensuring that access is granted only when required, adhering closely to the concept of tailored and context-based authorization in the Zero Trust paradigm.

Function	Optimal Requirements	How Strong DM Supprts
Visibility & Analytics	Agency maintains comprehensive visibility and situational awareness across enterprise by performing automated analysis over user activity log types, including behavior-based analytics.	The platform's extensive visibility extends to 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. 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.
Automation & Orchestration Capability	Agency automates orchestration of all identities with full integration across all environments based on behaviors, enrollments, and deployment needs.	StrongDM's automation capabilities extend across the entire identity and access lifecycle and diverse environments. The platform fulfills the Zero Trust principle of automated and orchestrated access management by dynamically responding to factors such as role changes, behavior, and deployment needs.
Governance Capacity	Agency implements and fully automates enterprise- wide identity policies for all users and entities across all systems with continuous enforcement and dynamic updates.	The StrongDM platform can implement and automate comprehensive identity policies for tech staff (internal and external contractors) across the entire organizational landscape. These policies undergo continuous enforcement and adaptive updates, aligning perfectly with the Zero Trust ethos of perpetual policy implementation.

5.3 Networks

Networks are the third pillar of the ZTMM. This refers to "an open communications medium including typical channels such as agency internal networks, wireless networks, and the Internet as well as other potential channels such as cellular and application-level channels used to transport messages."

In terms of access management, this involves treating each application uniquely by the network based on its access, priority, reachability, and connections (dependency services and pathways).



StrongDM & Networks

Function	Optimal Requirements	How Strong DM Supprts
Network Segmentation	Agency network architecture consists of fully distributed ingress/ egress micro-perimeters and extensive micro-segmentation based around application profiles with dynamic just-in-time and just-enough connectivity for service-specific interconnections.	StrongDM aligns with the highest level of network segmentation by enabling 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.
Network Traffic Management	Agency implements dynamic network rules and configurations that continuously evolve to meet application profile needs and reprioritize applications based on mission criticality, risk, etc.	StrongDM implements dynamic and evolving network rules and configurations. These configurations are tailored to meet the specific requirements of applications, factoring in mission criticality and risk. This level of agility in network traffic management ensures optimal resource utilization while adapting to changing operational demands. StrongDM Gateways are specifically hardened to be exposed for ingress for StrongDM clients to connect. StrongDM will only accept connections from a StrongDM client that was first authenticated and authorized via the StrongDM Control Plane for access.
Traffic Encryption (Formerly Encryption)	Agency continues to encrypt traffic as appropriate, enforces least privilege principles for secure key management enterprise- wide, and incorporates best practices for cryptographic agility as widely as possible.	Within the context of traffic encryption, StrongDM continues to uphold encryption practices where appropriate. Moreover, the platform enforces least-privilege principles for secure key management. This commitment to cryptographic best practices and agility ensures secure communication while maintaining the ability to adapt to evolving cryptographic standards.
Network Resilience (New Function)	Agency integrates holistic delivery and awareness in adapting to changes in availability demands for all workloads and provides proportionate resilience.	StrongDM ensures network resilience by flexibly adjusting to changing availability demands across workloads. This proportionate resilience guarantees a reliable infrastructure.
Visibility & Analytics Capability	Agency maintains visibility into communication across all agency networks and environments while enabling enterprise-wide situational awareness and advanced monitoring capabilities that automate telemetry correlation across all detection sources.	StrongDM supports this requirement by providing complete audit data for all session types across all environments enabling threat hunting and telemetry correlation in your system of choice.

Function	Optimal Requirements	How Strong DM Supprts
Automation & Orchestration Capability	Agency automates orchestration of all identities with full integration across all environments based on behaviors, enrollments, and deployment needs.	StrongDM's approach aligns with the ideal by leveraging infrastructure-as-code principles for network definition and management. This involves utilizing automated change management methods to ensure the network architecture is in harmony with evolving operational requirements. Automated initiation and expiration of network configurations facilitate real-time adaptability.
Governance Capacity	Agency implements enterprise-wide network policies that enable tailored, local controls; dynamic updates; and secure external connections based on application and user workflows.	StrongDM supports optimal governance capabilities by implementing dynamic, tailored policies that move closer to the actor and resource and transition away from perimeter-based protections.

About StrongDM

StrongDM is a Dynamic Access Management platform that centralizes privileged access for all technical users to every resource in your infrastructure on-premises and in the cloud. Security teams have complete visibility into every keystroke to enhance security and compliance postures and end users enjoy fast intuitive access to resources they need. Connect with us on LinkedIn, X (formerly Twitter), Facebook, YouTube or head to www.strongdm.com to learn more.