Silverfort

Comply with Zero Trust Maturity Model (ZTMM) requirements with Silverfort

Whitepaper

Executive summary

The Zero Trust Maturity Model (ZTMM) was developed by the US Cybersecurity and Infrastructure Security Agency (CISA) in 2023 to guide organizations in designing and implementing Zero Trust Architecture (ZTA) principles. Originally created for US federal agencies in alignment with Executive Order 14028 and OMB Memorandum M-22-09, ZTMM framework has been implemented across finance, healthcare, energy sectors.

The framework defines gradient implementation of five key pillars: Identity, Devices, Networks, Applications and Workloads, and Data, helping organizations in identity security posture improvement. The main goal of ZTMM is to facilitate organizations shifting their approach from implicit trust to zero trust principles - enforcing access controls based on identity, context, and risk.
ZTMM supports organizations in improving their identity security posture, increasing resilience, and implementing principle of least privilege across their hybrid environments.

Addressing the identity security aspects of ZTMM

The framework identifies **Identity** and **Applications & Workloads** as foundational pillars for enforcing strong access control and reducing the attack surface. The four maturity stages, including **Traditional**, **Initial**, **Advanced**, and **Optimal**, represent a gradient progression from manually configured and static controls to fully automated, adaptive security.

By following ZTMM guidelines, organizations can enhance visibility and identity governance, apply dynamic access policies based on automated triggers, strengthen their identity security posture against credential-based attacks, lateral movement and privilege escalation.

Silverfort Identity Security Platform

Silverfort enables organizations to implement Zero Trust principles across hybrid environments by enforcing strong authentication and dynamic access controls. The platform extends security controls like multi-factor authentication (MFA), risk-based authorization, and continuous identity verification to all users, devices, and services – across on-prem, cloud, and hybrid systems.

By integrating with existing Identity and Access Management (IAM) infrastructure, Silverfort unifies access visibility and control without requiring agents or proxies. It helps organizations progress through ZTMM maturity stages by preventing credential compromise, lateral movement, and unauthorized application access – supporting least privilege, just-in-time access, and secure application workflows at scale.

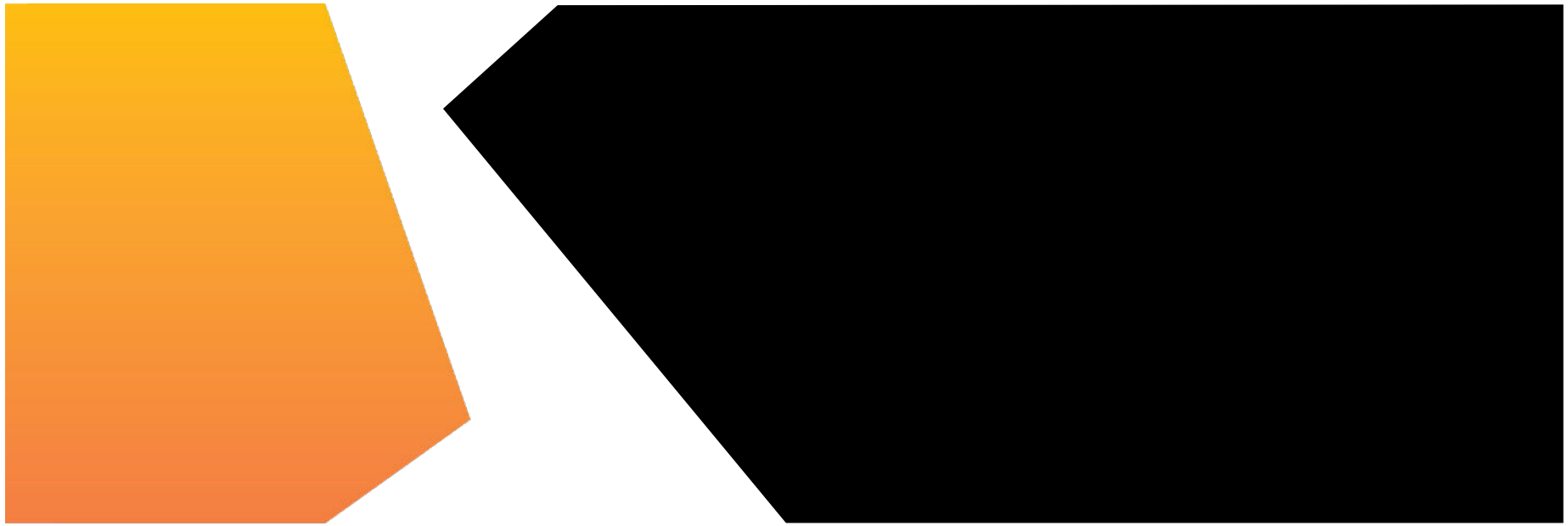
Silverfort Identity Security Platform Highlights

Multi-Factor authentication
Extend MFA protection to command-line access, legacy apps, IT infrastructure, and other critical resources that couldn't be protected before.

Detect and respond to identity threats
Detect common credential access, privilege escalation and lateral movement attacks, and respond automatically with real-time blocking.

Securing privileged users
Discover, classify, and enforce least privilege and Just-In-Time (JIT) access policies for all your privileged users.

Continuous monitoring
Gain comprehensive visibility into all authentication and access attempts, monitor and review them continuously to detect anomalies and prevent malicious access in real-time.



Compliance table: Silverfort alignment to ZTMM's requirements

Identity

The Identity pillar focuses on ensuring that users and entities have access to the right resources at the right time for the right purpose - without granting excessive permissions. It emphasizes integrating identity, credential, and access management solutions to enforce strong authentication, enable context-based authorization, assess identity risk, and enhance visibility across all enterprise identities.

ZTMM Function	ZTMM Regulation		Silverfort Security Controls
	Advanced	Optimal	
Authentication	Agency begins to authenticate all identity using phishing-resistant MFA and attributes, including initial implementation of password-less MFA via FIDO2 or PIV (Personal Identity Verification).	Agency continuously validates identity with phishing-resistant MFA, not just when access is initially granted.	Silverfort authenticates each user's identity by enforcing strong MFA across all resources and access interfaces, including those that don't natively support modern authentication protocols. Silverfort can authenticate users in real-time, providing continuous protection against phishing and other cyber threats.
Identity Stores	Agency begins to securely consolidate and integrate some self-managed and hosted identity stores.	Agency securely integrates their identity stores across all partners and environments as appropriate.	Silverfort automatically discovers all user accounts in your environment, including privileged accounts and non-human identities, and provides real-time visibility inro all their activity. By enforcing pre-defined access control policies, you can prevent any malicious activity from user accounts and deny their access to any critical resources within your on-prem, cloud or hybrid environment. Silverfort can enforce least privilege access and just-in-time (JIT) policies to ensure that users only have access to critical resources when necessary and only that is required for their roles.
Risk Assessments	Agency determines identity risk with some automated analysis and dynamic rules to inform access decisions and response activities.	Agency determines identity risk in real time based on continuous analysis and dynamic rules to deliver ongoing protection.	Silverfort provides full visibility and continuous monitoring and risk analysis of all authentication and access attempts, including sources, destinations, risk levels, and more. To ensure that if an access attempt deviates from normal behavior, the policy will provide alerts and/or deny access. With Silverfort you can configure a policy that requires the end-user to verify authentication from every device you are working from. If a user denies an MFA, and there are other risk indicators involved, Silverfort creates a User Denied Suspicious Authentication incident that can be investigated and mitigated.

ZTMM Function	ZTMM Regulation		Silverfort Security Controls
	Advanced	Optimal	
Access Management (New Function)	Agency authorizes need-based and session-based access, including for privileged access request, that is tailored to actions and resources.	Agency uses automation to authorize just-in-time and just-enough access tailored to individual actions and individual resource needs.	With Silverfort, you can automatically discover and classify all privileged accounts based on user activity. This enables you to gain comprehensive visibility into all privileged accounts, cross-tier authentications, and access requests to identify whether regular accounts are being used with privileged intent. Silverfort allows you to implement Just-in-Time (JIT) access policies to ensure that privileged accounts only receive the necessary permissions when needed and for a limited duration.
Visibility and Analytics Capability	Agency performs automated analysis across some user and entity activity log types and augments collection to address gaps in visibility.	Agency maintains comprehensive visibility and situational awareness across enterprise by performing automated analysis over user activity log types, including behavior-based analytics.	Silverfort provides centralized visibility into every authentication and access request across all users and resources. With Silverfort's comprehensive audit logs of all authentication and access activities across all systems, you can gain detailed records of user actions, including logins, access attempts, and privileged account usage, enabling real-time monitoring, analysis, and reporting of unauthorized or suspicious behavior. These logs are centrally stored and can be integrated with SIEM tools for enhanced investigation and compliance reporting, ensuring full visibility into system activity for security audits.
Automation and Orchestration Capability	Agency manually orchestrates privileged user identities and automates orchestration of all identities with integration across all environments.	Agency automates orchestration of all identities with full integration across all environments based on behaviors, enrollments, and deployment needs.	Silverfort continuously monitors all user activities and access requests across the environment. This monitoring ensures that any changes in access rights or user roles are promptly detected. When a user leaves the organization, Silverfort's access policies will revoke all access for that user. This will prevent the user from gaining access to any resources.
Governance Capability	Agency implements identity policies for enterprise-wide enforcement with automation and updates policies periodically.	Agency implements and fully automates enterprise-wide identity policies for all users and entities across all systems with continuous enforcement and dynamic updates.	Silverfort provides centralized access control policy enforcement on each data access attempt, based on the administrator's policy settings and configurations. With Silverfort, administrators can configure and apply access control policies based on specific user roles, risk scenarios, and organizational security policies. These policies can enforce alerting, MFA, or block access upon insecure authentication to protected systems.

Applications & Workloads

The Applications & Workloads pillar focuses on securing applications with granular access controls, integrated threat protections, and secure delivery practices. Organizations are encouraged to make applications accessible to authorized users over public networks, adopt DevSecOps and CI/CD best practices, and treat applications as externally facing to strengthen security and resilience.

ZTMM Function	ZTMM Regulation		Silverfort Security Controls
	Advanced	Optimal	
Application Access (Formerly Access Authorization)	Agency automates application access decisions with expanded contextual information and enforced expiration conditions that adhere to least privilege principles.	Agency continuously authorizes application access, incorporating real-time risk analytics and factors such as behavior or usage patterns.	Silverfort enables you to manage and secure access to SaaS applications by authorizing and monitoring all connections through identity-based policies and real-time monitoring. It centralizes control via managed access points, enforces MFA, and secures privileged access, ensuring only authorized users can remotely access systems, with all activities closely monitored and documented.
Application Threat Protections (Formerly Threat Protections)	Agency integrates threat protections into all application workflows, protecting against some application-specific and targeted threats.	Agency integrates advanced threat protections into all application workflows, offering real-time visibility and content-aware protections against sophisticated attacks tailored to applications.	Silverfort integrates with all identity providers to seamlessly monitor all identity traffic and authentication activities in one place, including access to SaaS applications. With complete visibility across all user activities. Silvrefort's risk engine can determine the risk of every authentication, so organizations can detect and respond to potential security threats in real time - including blocking access of any accounts that display anomalous behavior, while alerting on any excessive access requests and detected malicious activity.

ZTMM Function	ZTMM Regulation		Silverfort Security Controls
	Advanced	Optimal	
Accessible Applications (Formerly Accessibility)	Agency makes most of their applicable mission critical applications available over open public network connections to authorized users as needed.	Agency makes all applicable applications available over open public networks to authorized users and devices, where appropriate, as needed.	Silverfort enforces access and security controls and their access requests to resources, including SaaS applications. By applying concrete security controls to all users, Silverfort helps prevent any authorized access in real time, ensuring only authorized users can gain access to specific SaaS applications.
Visibility and Analytics Capability	Agency automates profile and security monitoring for most applications with heuristics to identify application-specific and enterprise-wide trends and refines processes over time to address gaps in visibility.	Agency performs continuous and dynamic monitoring across all applications to maintain enterprise-wide comprehensive visibility.	Silverfort provides centralized visibility into every authentication and access request across all users and resources, including SaaS applications. With Silverfort's comprehensive audit logs of all authentication and access activities across all applications, you can gain detailed records of user actions, including logins, access attempts, and privileged account usage, enabling real-time monitoring, analysis, and reporting of unauthorized or suspicious behavior. These logs are centrally stored and can be integrated with SIEM tools for enhanced investigation and compliance reporting, ensuring full visibility into system activity for security audits.

About Silverfort

Silverfort secures every dimension of identity. We deliver end-to-end identity security that is easy to deploy and won't disrupt business operations, resulting in better security outcomes with less work. Discover every identity, analyze exposures, and enforce protection inline to stop lateral movement, ransomware, and other identity threats.

Learn more