Silverfort and Microsoft Defender for Identity (MDI)

Silverfort and Microsoft provide unmatched real-time detection and prevention of identity threats in a unified manner, across all resources and environments.

Identity-based attacks frequently include a key component — the use of compromised credentials to move laterally to other resources. In an effort to prevent these attacks, Silverfort and Microsoft have partnered to deliver unmatched real-time detection and prevention of identity threats in a unified manner across all resources and environments.

MDI and Silverfort: Stopping Identity-Based Attacks

The integration between Microsoft Defender for Identity (MDI) and Silverfort provides organizations with real-time prevention capabilities in addition to their MDI capabilities.

MDI detects malicious activities targeting all user accounts, while Silverfort can respond by blocking these threats in real time. Through this collaboration of MDI and Silverfort's Identity Threat Detection and Response capabilities, organizations are able to strengthen their resilience to today's evolving threats, including account takeover, lateral movement, and ransomware propagation, while preventing them in real time without disruption.

How the MDI and Silverfort Integration Works

Whenever MDI detects a threat, such as compromised credentials being used in a “Pass the Hash” attack, the user risk level is raised, and an Entra ID (formerly Azure AD) Conditional Access policy is triggered. Silverfort automatically extends this policy to on-prem authentication as well as non-Entra ID authentications. In this manner, attacks can be prevented for all systems (even ones that do not support MFA or modern authentication, such as command-line tools, file shares, and critical IT/OT infrastructure).

This unique integration not only stops attacks in real-time but also drastically reduces false positive alerts. Silverfort leverages MFA as an ideal, least-intrusive protection mechanism. By utilizing MFA, the security team is removed from the initial threat response, while providing its security analysts with concrete, actionable information to identify and eradicate malicious activity easily.

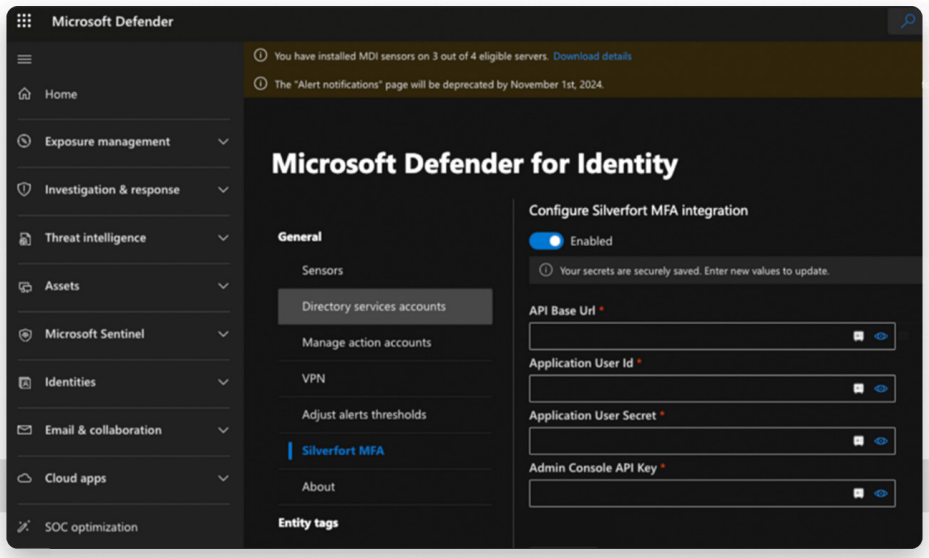
KEY BENEFITS

Extend Entra MFA
Apply MFA to on-prem legacy applications, command line access to workstations and servers, IT/OT infrastructure and other resources that couldn’t be protected before.

Prevent Lateral Movement
Gain proactive prevention of lateral movement attacks and ransomware propagation.

Response Without Disruption
Prevent compromised users from accessing resources while allowing legitimate users to prove their identity and avoid interruption.

Identity Zero Trust
Enforce granular authentication and access policies for any access to corporate resources, based on the user’s risk.



The Silverfort MFA is configured directly from Microsoft Defender for Identity. Under Identity Settings, select Silverfort MFA.