Silverfort | Microsoft

Silverfort for Microsoft 365 E5

Enhance Microsoft 365 E5 Security Products with Silverfort

Whether you're already fully deployed with multiple Microsoft 365 E5 security products or just starting, Silverfort provides identity security across on-prem, cloud, and edge environments.

By extending and enhancing your investment in Microsoft 365 E5 to resources and interfaces that couldn't be protected before such as legacy applications, on-prem servers, and more.

How Silverfort Empowers Microsoft 365 E5 Products

E5 Product	Silverfort + Microsoft
Entra ID P1/P2 Conditional Access & MFA	Extend Entra ID to on-prem, and other IdPs to allow unified policies in Entra ID conditional access drive decisions based on on-prem authentications
Entra ID Passwordless	Ability to extend Azure Passwordless authentication to on-prem resources (including legacy applications and command-line tools) for a unified user experience
Entra ID identity protection	Receive risk signal and indicators of identity compromise by Entra ID identity protection and leverage them for preventions methods like MFA on-prem
Entra ID PIM	Apply Entra ID PIM workflows to on-prem resources
Microsoft Defender for Endpoint	Remediate risks detected in MDE by invoking on-prem MFA, for example when a user has an endpoint that is compromised with malware
Microsoft Defender for Cloud Apps	Protect against risks that are detected by Microsoft Defender for Cloud Apps by triggering MFA for on-prem authentications. For example a user with compromised credentials attempts to delete data from a cloud app and an attacker uses the credentials to connect to on-prem file share and encrypt the data
Microsoft Defender for Identity	Mitigate identity-based attacks detected in MDI to trigger MFA for on-prem authentications, for example when a pass-the-hash attack occurs and an attacker captures a password hash and then passes it through for authentication and lateral access
Microsoft Defender for Office 365	Identify risks that are detected by MDO and trigger MFA for on-prem authentications, for example a user account is compromised and the attacker hacker attempts to send malware to another user in the organization to move laterally