

# Silverfort for Microsoft 365 E5









**Silverfort for Microsoft 365 E5 includes product integrations that help organizations consolidate their IAM across hybrid environments, extend identity protection and MFA to any asset, and simplify cloud migration**

Today's data breaches and ransomware attacks often include two key components – exploiting the endpoint and using compromised credentials to move laterally to additional resources. Silverfort and Microsoft have joined forces to deliver unmatched real-time detection and prevention of identity threats in a unified manner, across all resources and environments.

## 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 unified identity protection 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
 <p>Entra ID (formerly Azure AD) P1/P2 Conditional Access &amp; MFA</p>	<p>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</p>
 <p>Entra ID Passwordless</p>	<p>Ability to extend Azure Passwordless authentication to on-prem resources (including legacy applications and command-line tools) for a unified user experience</p>
 <p>Entra ID identity protection</p>	<p>Receive risk signal and indicators of identity compromise by Entra ID identity protection and leverage them for preventions methods like MFA on-prem</p>
 <p>Entra ID PIM</p>	<p>Apply Entra ID PIM workflows to on-prem resources</p>
 <p>Microsoft Defender for Endpoint</p>	<p>Remediate risks detected in MDE by invoking on-prem MFA, for example when a user has an endpoint that is compromised with malware</p>
 <p>Microsoft Defender for Cloud Apps</p>	<p>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.</p>
 <p>Microsoft Defender for Identity</p>	<p>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</p>
 <p>Microsoft Defender for Office 365</p>	<p>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</p>