

Unified Identity Protection

Extend MFA and identity Zero Trust to resources that couldn't be protected before

Silverfort is the first platform to deliver modern identity security across all corporate users, service accounts and resources, including legacy systems and command-line interfaces that are leveraged in more than 80% of data breaches and ransomware attacks, and were previously considered 'unprotectable'. Silverfort uses innovative agentless and proxyless technology that runs in the backend of the existing IAM infrastructure to enforce Multi-Factor Authentication (MFA), Identity Threat Detection and Response (ITDR) and Zero Trust policies across the hybrid environment and stop identity threats in real time.

Solve the identity protection challenges that matter most



Extend MFA to resources that couldn't be protected before

Extend MFA protection (including your existing MFA product) to critical resources without modifying them, including legacy applications, command-line access tools, file shares, IT infrastructure, industrial systems and many others.



Discover, monitor and protect your service accounts automatically

Gain immediate visibility into all service accounts (non-human identities), monitor and analyze their activity, and enforce policies that prevent anyone from using them outside of their intended purpose, without having to modify them.



Block ransomware spread and lateral movement in real time

Enforce adaptive MFA policies on high-risk access, including command-line tools that attackers frequently use like PowerShell, PsExec and WMI, to prevent ransomware spread and limit its impact to the initially compromised machine only.



Restrict insecure access with authentication firewall

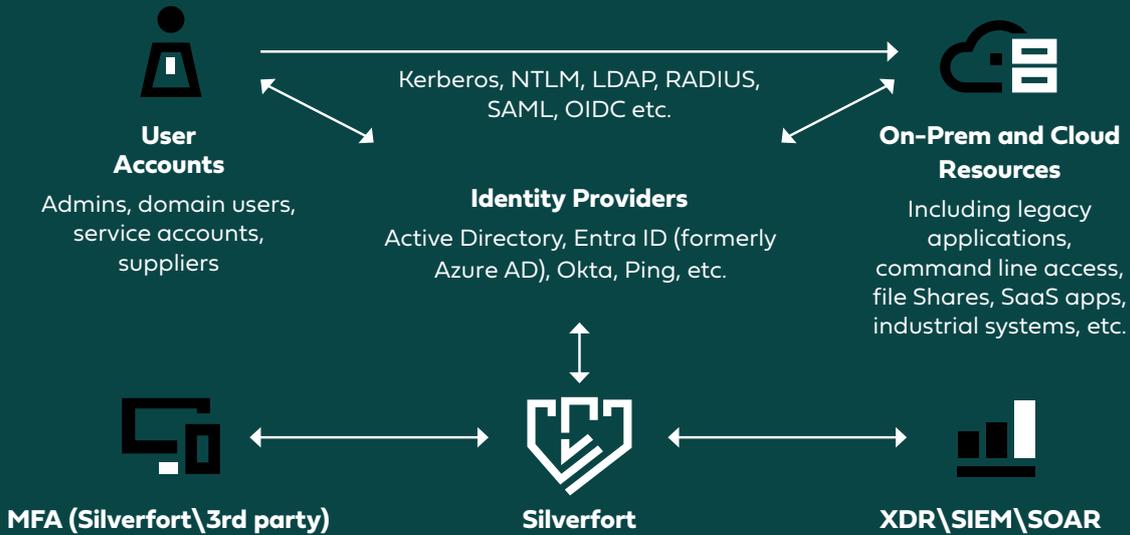
Harden your security posture by preventing risky access of insecure protocols and users, enforce least privileged access policies to eliminate excessive access, and block malicious access in detected breaches with a single click.

Meet the Cyber Insurance MFA and Privileged Access Requirements

Silverfort helps customers comply with the new cyber insurance requirements for MFA, PAM and service account protection across all corporate assets, including ones that were too difficult or time-consuming to protect with any other solution, without any modification or code change.

How Does It Work?

Silverfort enforces protection from the backend of your existing IAM infrastructure, including legacy directories like AD, using unique integrations that allow Silverfort to act as a 'second opinion'. This enables Silverfort to monitor all access activity, detect identity threats in real time (and report them to your XDR/SIEM/SOAR), and enforce security controls that these directories are often missing, such as MFA, before instructing the original directory whether to approve the access. Thanks to this innovative architecture, no changes are required to the various servers and applications.



Trusted by hundreds of enterprises globally



"Silverfort's innovative solution simplifies and expedites the process of implementing secure authentication for large enterprises without the need for system modifications, so enterprises can save time and money."

William Woo
Group CIO, Singtel



"Silverfort is the only solution that can prevent ransomware attacks by enforcing MFA on the command line access tools these attacks use to propagate in the network."

Billy Chen
Director of Cyber Security, RWC



"Silverfort protects all of our on-prem resources, cloud resources, custom apps and service accounts, which is amazing - they lived up to their word. I never thought we'd be able to do that."

Jim Nonn
CIO, Egan

Silverfort + Microsoft: a strategic alliance for identity protection



"The integration with Silverfort allows customers to extend the power and flexibility of Azure AD to many additional resources and applications across hybrid and multi-cloud environments, and unify their identity management and protection on Azure AD."



Sue Bohn, Partner Director, Microsoft Identity Division at Microsoft