SILVERFORT

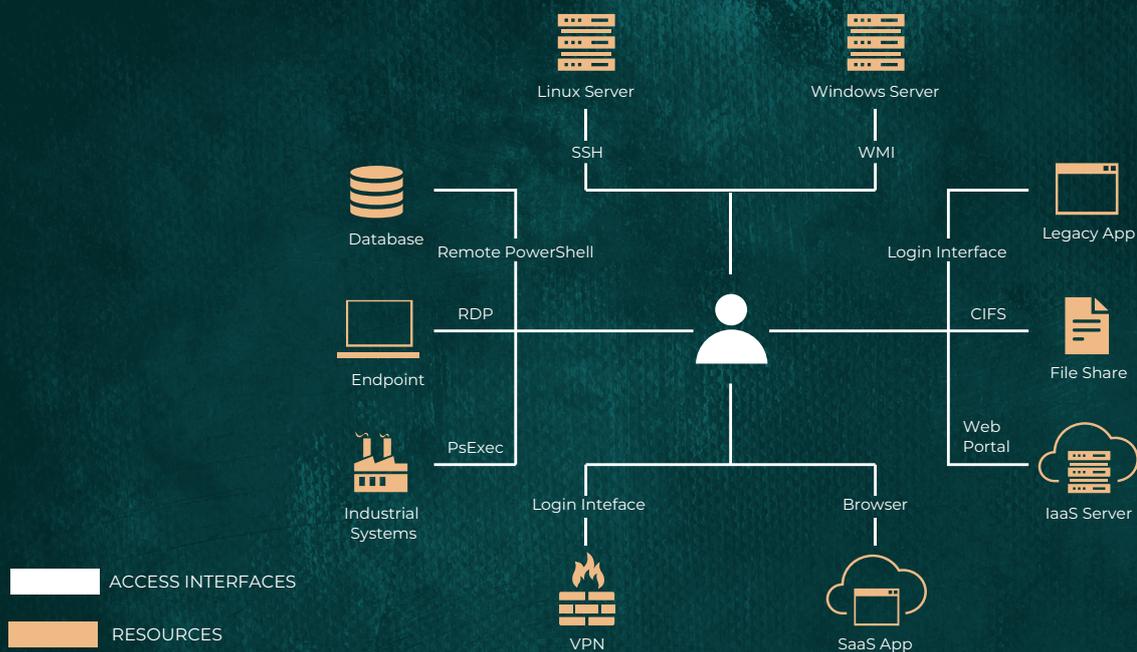# Silverfort MFA: Protect the Unprotectable

Extend MFA to all cloud and on-prem resources, including ones that couldn't be protected before

Silverfort utilizes agentless and proxyless technology to apply MFA to any resource and access interface across the on-prem and multi-cloud environments. This includes assets that could never have been protected with MFA before, including legacy and homegrown applications, command-line access tools, industrial and healthcare systems, file shares, databases, and more. Use Silverfort as your ultimate MFA solution or leverage its native integrations with leading providers to extend their protection to the entire environment.

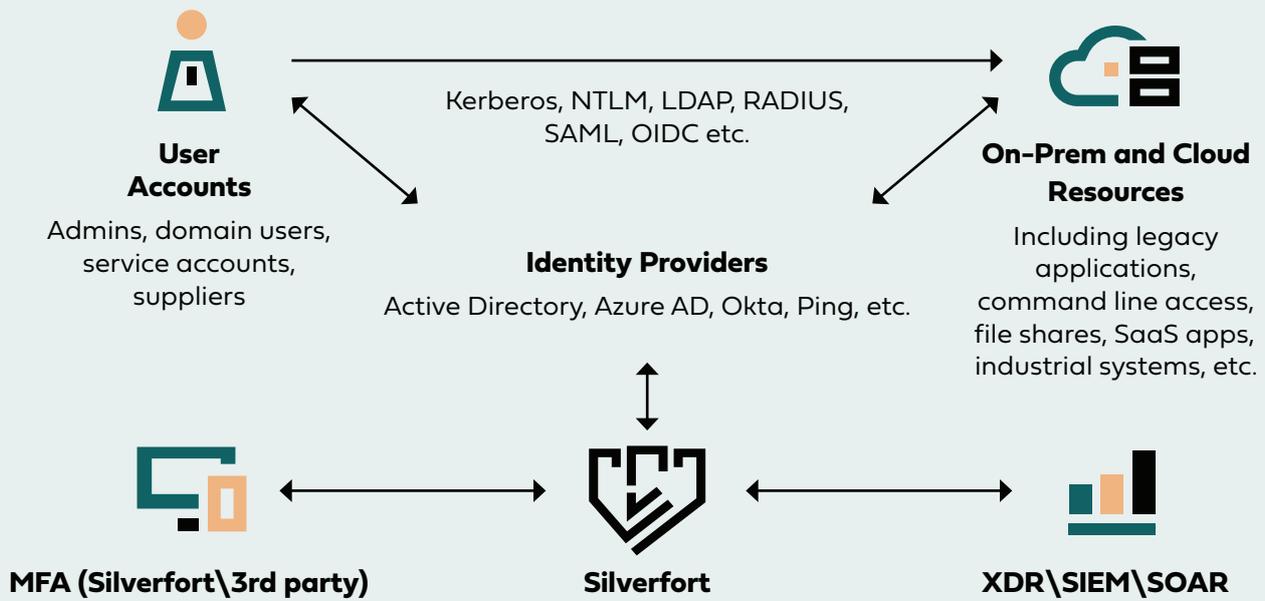## Protect all your resources and access interfaces

- Homegrown applications
- Legacy systems
- Admin access tools
- File systems and databases
- VPN

- IT Infrastructure
- Desktop login
- RDP & SSH
- SaaS applications
- VDI & Citrix

360 MFA Coverage Across all Resources and Access Interfaces

Linux Server — SSH
Windows Server — WMI

Database
Remote PowerShell
Login Interface
Legacy App

Endpoint
RDP
CIFS
File Share

Industrial Systems
PsExec
Web Portal
IaaS Server

Login Inteface
Browser

VPN
SaaS App

ACCESS INTERFACES
RESOURCES

SILVERFORT

www.silverfort.com

How Does It Work?

The Silverfort platform natively integrates with all IAM solutions within the hybrid environment to provide real-time monitoring and risk analysis for every user authentication and access request, including ones made by external vendors. Silverfort determines whether to allow, block, or require MFA and If MFA is required, Silverfort notifies the MFA solution to push an MFA notification to the user. Based on the user's response, Silverfort instructs the identity provider on whether the access request can be granted.

User Accounts

Admins, domain users, service accounts, suppliers

Kerberos, NTLM, LDAP, RADIUS, SAML, OIDC etc.

On-Prem and Cloud Resources

Including legacy applications, command line access, file shares, SaaS apps, industrial systems, etc.

Identity Providers

Active Directory, Azure AD, Okta, Ping, etc.

MFA (Silverfort\3rd party)

Silverfort

XDR\SIEM\SOAR

Choose Your Silverfort Implementation Path

Replace Your Existing MFA Solution

Implement Silverfort's unified identity protection platform as the single MFA solution in your environment for all on-prem and cloud resources. This provides both comprehensive protection and delivers simpler maintenance and significant savings.

Complement the MFA Solution you have in Place

Keep your existing solutions in place and implement Silverfort for the resources that couldn't have been protected before. While not reducing operational complexity, this delivers immediate coverage to all the resources that are currently exposed and ensure end-to-end MFA protection in your environment.

Consolidate the MFA of Your Choice

Choose one of your MFA solutions as the prime provider and use Silverfort to extend this solution to all the resources it doesn't natively support. This provides you the opportunity to offer your employees a consistent user experience regardless of what resource they attempt to access