SILVERFORT

360° MFA Protection for OT Environments

Enforce adaptive access policies and advanced MFA protection across all OT resources, including those that couldn't be protected before

Operational technology (OT) is more connected than ever, with a rapidly increasing number of OT environments shifting from local user access to HMI, engineering workstations, and production apps, to centralized SSO via Active Directory (AD). While the productivity advantages of this transit are clear, it also exposes such OT environments to a wide range of identity threats that leverage the same AD infrastructure for malicious resource access. Silverfort addresses this security gap by providing full MFA protection to any resource within an AD managed OT network.

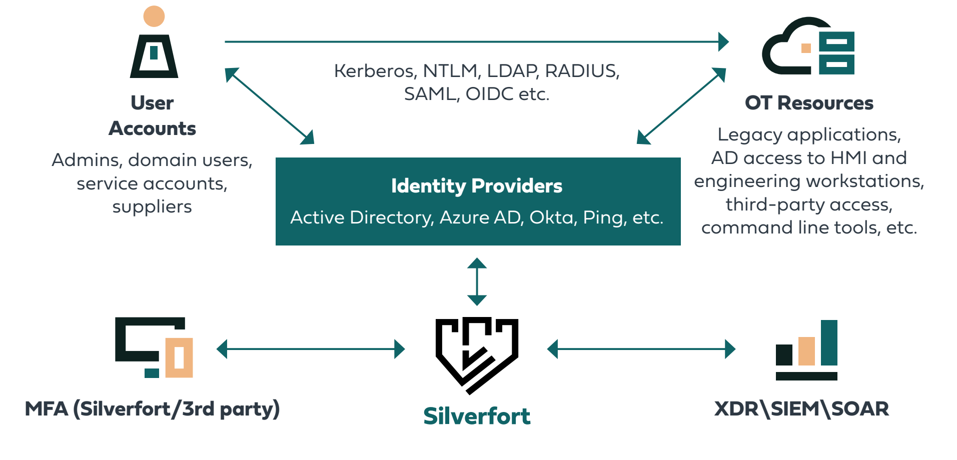
OT Networks Encounter a Dead End in Complying with MFA Requirements

Industrial organizations face immense challenges in complying with various standards such as NIST, NERC-CIP, and IEC-62443, that require the implementation of MFA across all their resources. However, their legacy applications that run critical production processes, were created long before MFA technology was widely available, so the only way to subject them to MFA protection is to modify their code which for most organizations is not an option. This results with result with a critical compliance gap that no traditional security solution can address.

Silverfort Extends MFA to any OT Resource

Silverfort's integration with AD enables it to monitor, analyze and enforce MFA protection on any AD authentication, obviating the question of whether the OT application natively supports MFA or not. As long as the application's authentication is carried out in AD Silverfort's MFA can protect it. Once a user attempts to access the application, an access request is made to AD that forwards it to Silverfort, which can challenge this user with MFA to verify its identity, either via a mobile app, or, if it's an air-gapped network, with a hardware token. In that manner, MFA becomes applicable to any resource within the OT network, including those that could never have been protected before.

How Does it Work?



User Accounts
Admins, domain users, service accounts, suppliers
Kerberos, NTLM, LDAP, RADIUS, SAML, OIDC etc.
OT Resources
Legacy applications, AD access to HMI and engineering workstations, third-party access, command line tools, etc.
Identity Providers
Active Directory, Azure AD, Okta, Ping, etc.
MFA (Silverfort/3rd party)
Silverfort
XDR\SIEM\SOAR

KEY BENEFITS

Protect the 'Unprotectable'
Extend MFA and access policies to any OT resource, including systems that could not be protected before.

Real-Time Protection
Identify and prevent identity-based attacks which utilize compromised credentials, across your OT environments.

Non-Intrusive Architecture
Monitor and control all authentication traffic without agents, proxies, or modification of OT application code.

Secure Productivity
Enable secure usage of AD, leveraging the benefits of SSO access while maintaining full protection against identity threat.